CONTROL IN THE PRESENCE OF AN INTELLIGENT JAMMER WITH LIMITED ACTIONS

BY

ABHISHEK GUPTA

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Aerospace Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2011

Urbana, Illinois

Advisers:

Professor Tamer Başar
Assistant Professor Cédric Langbort

ABSTRACT

In this thesis, we consider three different problems related to control using communication channel as a medium to transfer control signal in a networked control system. In particular, we are interested in control in the presence of an intelligent and strategic jammer who is maliciously altering the control signal or observation signal in the communication network connecting the controller and the plant.

The first formulation considers a dynamic zero-sum game between a controller and a jammer for two different scenarios. The first player acts as a controller for a discrete time LTI plant, while the second player acts to jam the communication between the controller and the plant. The number of jamming actions is limited, which captures the energy constraint of the jammer. In the first scenario, the state of the plant is unconstrained, while in the second scenario, the state of the plant is constrained by a threshold at all time steps, and both the jammer and the controller try to maintain the state of the plant below that threshold. We determine saddle-point equilibrium control and jamming strategies for these two games under the full state, total recall information structure for both players, and show that the jammer acts according to a threshold-based policy at each decision step. Various properties of the threshold functions are derived and complemented by numerical simulation studies.

The next problem considers a model of stealthy attack on a networked control system by formulating a static zero-sum game among four players. The three players constitute a team of encoder, decoder and controller for a scalar discrete time linear plant, while the fourth player acts to flip the bits of the binary encoded observation signal of the communication channel between the plant and the controller. We are interested in characterizing the possible encoding/decoding/control defense strategies available to the controller and for simplicity, we model it for a scalar discrete time system with only one time step. We further assume that the communication channel has finite bandwidth, and that the observation and control signals have finite codelengths. We determine the saddle-point equilibrium control and jamming strategies for this game when the controller's strategy space is restricted to quantization-based policies, and show that the resulting performance compares favorably to universal lower bounds obtained from rate-distortion theory. We also provide a necessary and sufficient condition on the minimum number of bits that are required to drive the cost to zero for this one step control problem in the presence of a jammer.

There are three births of a man; first as a child, second after education and third after death.

Dr. S. Radhakrishnan

Indian Philosophy - Vol. I

To my parents, sister Shubham and brother Shubhankar

ACKNOWLEDGMENTS

I would like to thank my advisors Prof. Tamer Başar and Prof. Cédric Langbort for their constant advice and feedback throughout my research. Our meetings were insightful and thought provoking and I have learned a lot about research from them. I could deepen my understanding of control theory, refresh motivations towards research and acquire new insights through these meetings.
Prof. Langbort has always amazed me with his patience. His constructive feedback on various facets of research have made my thought process more structured and clear. Prof. Başar's book - "Dynamic Non-cooperative Game Theory" has been an excellent reference for me throughout my research. I am also indebted to the professors at IIT Bombay and here at UIUC, from whom I have learned a lot in the classes as well as through personal interaction during leisure hours.

I would like to acknowledge AFOSR Grant FA9550-09-1-0249 and AFOSR grant for MURI - "Multi-Layer and Multi-Resolution Networks of Interacting Agents in Adversarial Environments" for full support during my Master's degree.

I am very thankful to my research group Nathan, Ali, Sourabh, Takashi and Albert for helping me out at various stages of my research and being an excellent company. Ankur, Anupama, Ashish, Aditya, Darshan, Zeba and Nihal are great friends and a constant source of motivation in the past two years. I couldn't have done so much without their support. Himanshu, Harshad, Amod, Ankita, Aditi and Vandana have been always supportive which makes me lucky to have them as my friends. I am deeply indebted to my parents, sister and brother for their love and support in my life.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Communication theory mainly deals with exact reconstruction of a message which has been transmitted from a distant location. A typical communication task involves encoding the message into bits, sending it across a wired/wireless channel and decoding the received bits which may be erroneous due to inherent noise in the medium. Control theory, on the other hand, assumes in general that the control signal received at the plant end from the controller is free of errors, and the received signal is applied to the plant.

Using communication channel as a medium to transfer control signal restricts the controller's ability to stabilize the system or achieve optimality in closed loop. Limitations of a communication channel include limited data rate and channel capacity, stochastic packet drops and delays, and bounded signal-to-noise ratio. The adverse effects of such communication channel-induced limitations on control systems have been intensively studied in the past decade. For example, a number of papers have considered the minimum channel rate necessary for stabilization (see, e.g. [1, 2, 3]) or achieving optimal quadratic closed-loop performance [4, 5, 6].

In some communication protocols, acknowledgement packets are sent by the receiver to the transmitter to acknowledge the successful error-free transmission of the message. In control systems, when such acknowledgements are sent by the receiver to the transmitter[1], then it results in a classical information pattern for the controller and separation holds for the optimal controller in the classical linear-quadratic Gaussian problem. Non-classical information patterns arise in the case when the acknowledgement is not sent to the controller or the plant (see, e.g. [7, 8]). In such cases, the optimal control policy for the linear-quadratic Gaussian problem has no closed form solution and is a non-linear function of state.

Delay may occur in the communication systems if the message is to be transferred error-free across the channel or the message to be transferred has long codelength. In fact, most of the proofs of information theory which bounds the probability of error in the transmission of a message rely on arbitrarily large codelength, which entails large delays. Delay is typically directly proportional to codelength for a message - larger the codelength, larger is the delay associated with the transfer of message. Typical communication process can tolerate some delay as long as the message is transmitted error-free (would it matter to you if an email sent to you comes after a delay of say, one minute?). However, the performance of the control systems degrades rapidly with an increase in delay in transferring control or observation signal. Delay can increase the cost to the controller beyond an acceptable level or even worse, make the system unstable.

Most of the work in the field of networked control system has concentrated on the problem where the channel behavior is assumed independent of the controller's action or plant's state. In papers [4, 5, 9, 10], the channel induced limitations like dropping of control and observation packets are posed as a Bernoulli i.i.d.

[1]Here, receiver or transmitter may be a controller or a plant.

process which are uncorrelated in time. However, this is not true in the case where a malicious agent is trying to intentionally and strategically drop the control signal or alter the data in the communication network to deceive the controller. Such a scenario may arise in the battlefield where the enemies frequently jam to disrupt the communication channel or in large industrial networks where the data sent through wireless channels may be intercepted by malicious intruders.

In the absence of appropriate security measures, networked control systems are highly vulnerable to attack. Two types of attack on such systems have been considered in the past, namely denial of service (DoS) attack and deception (or integrity) attacks [11, 12, 13]. Under DoS attack, the communication link is jammed in order to break the information exchange between the subsystems, while in deception attacks, the data of the subsystems are tampered with in order to deceive the controller and harm the system.

These strategic moves by an antagonistic agent not only correlate the loss of information across time, but they also couple them with state of the system in cases where the antagonist has access to the state information. Of course, the problem formulation and the corresponding solution is dependent on the constraints on the action set and information structure of the antagonist in the system.

In addition to attacks on control systems by altering the crucial data, attacks have been reported in which the enemy hacks the system to obtain crucial data [14] or infect the software of control system with worms like STUXNET [15, 16]. However, these attacks are out of the realm of the study done in this thesis. Analysis of these attacks and measures to prevent such attacks require a complete understanding of communication, controls, computing, cryptography, security in wireless systems and their interplay from a systems-theoretic viewpoint and for a specific cyber-physical system. We consider very specific attacks in this thesis and more importantly, our analysis is done in a game-theoretic framework.

In the thesis, we consider three problems which arise in networked control systems. The first two problems deal with a strategic adversary who maliciously drops the control signal in order to cause harm to the system by increasing the cost to the controller, while the third problem deals with the jammer altering the observation signal for a one step control problem.

The first problem models the adversary as a jammer, who is maliciously trying to drop the control packet in order to increase the cost to the controller by using a finite number of jamming actions over a horizon of N time steps. This constraint on the number of jamming actions is similar to that introduced in [17, 18] in the case of optimal control (without an adversary), and in [19] in the case of estimation (again without an adversary). It is introduced in the present problem to capture the fact that, since jamming is a power intensive activity and available energy on-board a jammer is typically limited, continuous action throughout the entire decision horizon is not possible. The second problem introduces a safety critical observation constraint on the system, which both the controller and the jammer strive to maintain.

However, in digital systems, real numbers need to be quantized and binary codewords are sent across a channel. Limited bandwidth also prohibits the controller to send large amount of data over the network within a short span of time. This means that the quantization bin cannot be made arbitrarily small, so as to emulate the process of sending real numbers in finite time. Hence, in the third problem, we consider the scenario where the observation and control signals are sent in binary codewords with limited codelengths. The jammer, instead of blocking the signal completely, can only flip a limited number of bits in the codewords to corrupt the data. Jammer's role is similar to a binary symmetric channel, but is different in the sense that the jammer flips the bit deterministically and strategically to alter the data.

Let us first glance over the main references in the field of networked control systems involving wireless

communication as a medium to transfer information.

1.1 Previous Work

1.1.1 Control over Communication Channels

One of the first papers to consider control and observation with communication constraints is [20]. In this paper, Borkar and Mitter considered optimal control of a stochastic LQG discrete-time system with finite alphabet codeword and a constant delay between the plant and the controller. They showed that instead of quantizing and transmitting the state, if the plant encodes and transmits the innovation process along the lines of [21] in the unquantized case, then the controller has separation property[2]. Since then, a lot of research has been done in understanding the effect of quantization, packet losses, delay and limited data rate on the observability, stabilizability, control policy and corresponding system performance.

One of the problems associated with wireless channels is packet losses. In [9], the problem of Kalman filtering with intermittent observation is considered. In this scenario, the observation vector is received intermittently (modeled as an i.i.d. Bernoulli process) at the filter. The authors derived necessary and sufficient conditions on the packet arrival probability under which the second moment of the error in the estimate is bounded. The authors of [4, 5] considered the problem of LQG control over channels where the packet drop across the channel is modeled as i.i.d. Bernoulli process. If the controller and the plant receive acknowledgement packets, like in TCP protocols of the internet, then they show that the separation property holds for the system. Moreover, they derived necessary and sufficient conditions under which the modified Riccati equation, which takes into account control packet losses, converges in such a scenario. When the acknowledgement packets are not sent to the controller and the plant, like in UDP protocols, then the separation property does not hold and the system has a non-linear control policy.

Many authors (see e.g. [1, 25, 3, 26]) considered the problem of minimum channel rate required for a linear discrete-time system to be stabilizable when the observation or/and control packets are sent across a communication channel with limited capacity. Nair et.al. [2] compared the relative impacts of delay, data rate, open loop instability and process noise on the steady state control performance and stabilizability of the plant. They also show that optimal controller for linear discrete-time systems features certainty equivalence property even if the state information is sent across a channel with delay. Yüksel and Başar [26] considered both the feedforward and the feedback channel to be noisy and shown that for an invariant distribution of the state, the packet drop probability of the feedback channel must be greater than or equal to the packet drop probability of the feedforward channel.

1.1.2 Security in Control Systems

Jamming attacks have been considered in wireless communication for a long time under different channel characteristics [27, 28, 29]. It is frequently employed in battlefield for blocking the enemy signal and disrupt their communication network. Not all jamming is intentional; for example, large scale jamming can happen

[2]For more information regarding certainty equivalence and separation property of a controller, the reader is referred to [22, 23, 24].

in upper atmosphere in the event of solar flares [30]. However, coordinated and planned malicious jamming attacks may result in a complete failure of the control system.

In control systems, cyber attacks have been considered in numerous papers [13, 11, 31, 32] and the references therein. Amin et. al. [11] considered a random DoS attack on a control system, which is equipped with a quadratic cost function and a scalar constraint on the state and input in a probabilistic sense. They restricted the control strategy to be affine in the entire history of estimate of the state and obtained optimal control for such an attack as a solution to a convex problem.

In contrast to the random attack model in Amin et. al. [11], we consider here a strategic attack, since we believe that the jammer has no incentive to randomize his strategy if he could launch a denial of service attack in a planned fashion across time and make use of the information available to him at each instant of decision step. This also allows us to put a limited energy constraint on the jammer, that of limited number of actions in the entire horizon. We also consider the control strategies as measurable mappings of the controller's information set, instead of restricting them to be affine in the history of estimate. However, these generalization in the model comes at a cost, since the analysis of such attacks is difficult even for scalar linear systems with quadratic cost.

1.2 Overview of Chapters

The first problem considered in this thesis is that of a jammer who is maliciously and strategically dropping the control packets in the communication network connecting the controller to the plant. The precise problem is formulated in Chapter 2. We modeled the communication as an analog channel, which can pass real numbers (in the form of control signal) over the network. This falls in the category of denial of service attack, in which an intelligent jammer jams the communication link between the controller and the plant. The jammer's goal was to optimally block the control signal by using a finite number of jamming actions over a horizon of N time steps. The restriction on the number of times the jammer can jam captures the limited on-board energy with the jammer.

Our formulation, detailed in Chapter 2, naturally results in a dynamic zero-sum game between the jammer and the controller. We show that saddle-point equilibrium strategies exist by computing the value function of the game at each time step of the game and use dynamic programming to compute the value functions. In particular, we show that the jammer saddle-point equilibrium strategy is threshold-based, which means that at every time step, the jammer jams if and only if the plant's state is larger than an off-line computable and time-varying threshold. We start by investigating the situation in Chapter 3, in which there is no constraint on the state or observation. In Chapter 4, we introduce a safety critical observation constraint for the controller as well as the jammer. Both strive to maintain the observation below this constraint with the jammer trying to increase the cost to the controller.

We then look into the problem where the jammer flips a limited number of bits in the codeword for observation in Chapter 5. The cost to the controller is chosen to be the probability with which the state goes out of the bounded interval in the next time step given that the state started from that bounded set at the beginning of the game. This is formulated as a static game between the team of encoder, controller and decoder against a jammer for a linear discrete-time system. This results in wrong observation signal to reach the controller, which may result in control being different from what was intended. The study in Chapter

5 falls within the class of deception attacks as described above. We provide a necessary and a sufficient condition on the number of bits required by the controller to keep the state bounded when the state starts from a bounded set.

The thesis concludes with the concluding remarks of Chapter 6, which also identifies some future directions of research.

CHAPTER 2

JAMMING ATTACKS

A wireless network is built upon a shared medium which is accessible to many others. This makes it easier for adversaries to launch an eavesdropping or a jamming-type attack. In eavesdropping, the attacker only steals the information which is being transfered over the communication channel. This gives an informational advantage to the attacker in a combat scenario. Jamming type attacks, on the other hand, affect the quality of the service to the authorized traffic.

Jamming may not always be intentional. Some natural events like solar flares may jam the communication link between satellites and the ground station. Another kind of jamming can occur if there is interference by other devices that operate at the same frequency band as the system under consideration. Sometimes, just changing the frequency at which the communication is takes place may be sufficient to avoid jamming due to interference. Changing frequency of communication may not always work when powerful natural events like solar flares jam the signal. Most often, it may also be difficult to distinguish between a malicious jammer and a source of interference. If the antagonist is adaptive and strategic, then changing the frequency is not an appropriate strategy and one needs to take into account its presence in any strategy development.

In networked control systems, intelligent jamming actions can disrupt communication among critical elements of a control system, resulting in failure of one or more actuators to act at the intended time. Hence, a jamming attack can severely restrict the ability of a control system to perform in the desired (and expected) fashion. Consequently, mechanisms are needed to cope with jamming attacks on control systems.

2.1 Problem Formulation

The class of problems considered in this formulation can be viewed as the standard discrete-time linear-quadratic-Gaussian (LQG) control problem with state feedback, but with one major difference: as a networked control system, the link connecting the output of the controller to the plant is unreliable due to the presence of adversarial jamming, with a possibility of the control signal being intercepted by the jammer and not reaching the plant. Instead of limiting the jammer's action through an energy constraint, we instead allow the jammer only M possibilities of interception in problem of horizon N, where $M < N$. Further, if the control signal is intercepted, that the input to the plant is *zero*. It would be possible to adopt an alternate formulation where whenever the control signal is intercepted, the actuator generates an input that is based on the most recently received control signal, but this will not be pursued in this thesis.

Using scalar system dynamics, the scenario above can be captured through the following mathematical

formulation: The state equation under adversarial jamming evolves as

$$x_{k+1} = Ax_k + \alpha_k u_k + w_k\,, \qquad k = 0, 1, ..., N-1\,, \tag{2.1}$$

where $x_k \in \mathbb{R}$ is the state of the plant, $u_k \in \mathbb{R}$ is the control signal, $\{w_k\}$ is a discrete-time zero mean Gaussian white noise process with variance σ_w^2 (i.e. $w_k \sim \mathcal{N}(0, \sigma_w^2)$), and x_0 is also a zero mean Gaussian random variable, with variance σ_0^2, and independent of the noise process $\{w_k\}$. The sequence $\{\alpha_k \in \{0, 1\}\}$ is the

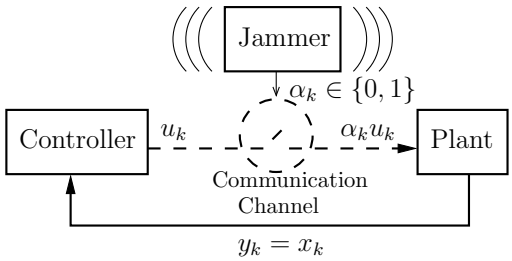


Figure 2.1: Control in the presence of an intelligent jammer.

control of the jammer, where $\alpha_k = 0$ means that the jammer is active at time k, whereas $\alpha_k = 1$ means that the jammer is inactive and the control signal reaches the plant. The assumption that the jammer is allowed to intercept at most M times (in a horizon of N), is captured by the jammer constraint $\sum_{k=0}^{N-1}(1-\alpha_k) = M$. Note that here we actually use an equality rather than an inequality because, as it will be clear from the analysis later, since the jammer does not incur any cost during each jamming instance, there is no incentive for it not to use all M allotments for interception. In fact, given any strategy for the jammer that involves fewer than M jamming instances, the optimum value of the cost function introduced below can be made strictly higher by allowing the jammer to intercept during any one of the non-jamming instances as dictated by the strategy.

The cost function associated with this problem is

$$J = E\left\{\sum_{k=0}^{N-1}(x_k^2 + \alpha_k u_k^2) + x_N^2\right\} \tag{2.2}$$

which is to be minimized by the controller and maximized by the jammer. Note that when the control signal is intercepted (that is, $\alpha_k = 0$), the controller accrues no cost for control.

This is clearly a zero-sum dynamic game, but to make the problem precise we have to specify the underlying information structure, and the equilibrium solution concept to be adopted. Toward this end, let $x_{[0,k]} := \{x_0, \ldots, x_k\}$,with a similar definition applying to $\alpha_{[0,k]}$, and let us introduce

$$I_0 := \{x_0\}\,, \quad I_k := \{x_{[0,k]}, \alpha_{[0,k-1]}\} \ \text{ for } k \geq 1$$

as the information available to both the controller and the jammer at time k. We introduce control policies (strategies) for the controller and the jammer as measurable mappings, $\{\gamma_k\}$ and $\{\mu_k\}$, respectively, from their information sets (which are the same for both) to their action sets; more precisely, $u_k = \gamma_k(I_k)$ and

$\alpha_k = \mu_k(I_k)$, where

$$\gamma_k : \mathbb{R}^{k+1} \times \{0,1\}^k \to \mathbb{R} \text{ and } \mu_k : \mathbb{R}^{k+1} \times \{0,1\}^k \to \{0,1\}\,.$$

We further restrict $\mu := \{\mu_0, \ldots, \mu_{N-1}\}$ to those maps that satisfy the jammer constraint, with $\alpha_k = \mu_k(I_k)$; let us denote the class of all such policies for the jammer by $\mathcal{M}$ and for controller by Γ. At each point in time, the controller has access to the current value of the state and recalls the past values, and also has full memory on whether any of the previous control signal transmissions were intercepted or not. This latter information could be made available to the controller through acknowledgement messages sent from the plant, as in TCP of the Internet. Likewise, the jammer has access to full state information, and recalls its past actions. There could, of course, be various variations of this information structure.

Now, given the information structure introduced above, and the feasible policies of the controller and the jammer, we rewrite the cost function as $J(\gamma, \mu)$, in terms of the policies γ and μ, and seek a pair $(\gamma^* \in \Gamma, \mu^* \in \mathcal{M})$ with the property:

$$J(\gamma^*, \mu) \leq J(\gamma^*, \mu^*) \leq J(\gamma, \mu^*) \quad \forall \gamma \in \Gamma, \mu \in \mathcal{M}\,.$$

This is a saddle-point solution for the underlying game, where the controller is the minimizer and the jammer the maximizer, and the order in which they determine their policies is immaterial (that is, the upper and lower values are equal). Of course, this has not been established as yet, and one of the goals of the thesis is to show that this is indeed the case, and also to obtain the saddle-point solution.

When $M = 0$, this is precisely the standard LQG problem with perfect state measurements, and for $M = N$, the controller signal is always intercepted and hence any pair of the form $(\gamma, 0)$ with $\gamma \in \Gamma$ is trivially a saddle-point solution; it is the *intermediate* case that is of interest.

2.1.1 Problem without State Constraint

In the problem formulated above, there is no hard bound on the state. Since the plant is modeled as a linear system, the state of the plant cannot grow arbitrarily large in finite horizon. Also, due to the cost on state, the controller always tries to keep the state as close to zero as possible.

Consider the scenario in which the initial state is large and the system is unstable. With high probability, the jammer will exhaust all his jamming actions at the beginning of the horizon, since it increases the cost for the state while the jammer is active as well as the control at later stages when jammer is inactive. This will increase the state to a very high value. However, in many applications, it is desired that the state be bounded, which motivates us put a hard constraint on the system state.

2.1.2 Problem with State Constraint

We assume that the reason why the jammer has an opportunity to intercept an incoming input signal from the controller is because the controller lets it do so, under particular circumstances. More precisely, we posit that it is willing to tolerate a small number of interceptions, say M in a decision horizon of length N ($M < N$), as long as it can ensure that no "critical event" will result from them. However, if it expects the safety critical constraints to be violated or observes more than M interceptions, the controller will (i) switch

to a different, secure actuation channel that is not accessible to the jammer and, (ii) apply the requisite input to ensure that the critical event does not occur. The result of this controller response behavior, which we assume to be known to both players, is that the jammer is in effect constrained to act at most M times, and so as to not violate the safety critical constraint, if it wants to have any influence on the outcome of the game.

For the sake of definiteness and simplicity, we restrict ourselves here (and in Chapter 4) to a safety critical constraint of the form

$$|E(x_{k+1}|I_k)| \leq \varrho \text{ for all } k = 0, ..., N-1 \tag{2.3}$$

for some pre-specified alert level ϱ. As a result, if, given its information state I_k, the controller expects the state at the next time step to leave the safe interval $[-\varrho, \varrho]$, it will in effect force the jammer to remain inactive, and apply the control input that achieves equality in (2.3).

While the description above results in a mathematically well-posed dynamic game in the sense that the controller's and jammer's strategy spaces are well-defined, there is still some ambiguity as to *why* the controller would decide to act in this way. If it does have the ability to isolate itself from the effects of the jammer's actions, why would it ever decide to join the game and tolerate any interception? Possible answers are: (i) that it may find it to its benefit to do so, e.g., if switching to the secure channel is particularly costly, or (ii) that, if it expects the basic control channel to be unreliable regardless of whether the packet drops are intelligently planned or not, it has no good reason to reject a channel subject to strategic jamming, as long as it cannot a priori distinguish the strategic and non-strategic situations (when the total number of interceptions is the same in both cases). In that case, requiring the jammer to use only M jamming instances can be seen as conferring it some degree of stealthiness, by allowing it to "masquerade" as a non-strategic channel.

Therefore, at the game level, there is a mutual cooperation between the controller and the jammer to keep the state bounded. The jammer is free to jam strategically in the region below the state constraint. It can be viewed as a scenario in which the jammer is reaping benefit from blocking the control signal, while maintaining the safety constraint in order to remain in the system and derive benefit from it for as long as possible.

2.2 Solution Approach

In order to establish the existence of and compute saddle-point equilibrium strategies, it is easiest to extend the game's state space so as to keep track of the jammer's options at a particular time step, and redefine the dynamics on this state space. An extented state of the dynamic zero-sum game defined by cost function J, information sets $\{I_k\}$ and evolution equation (2.1) is a triple $(x, s, t) \in \mathcal{E} := \mathbb{R} \times \{0, ..., M\} \times \{0, ..., N\}$, where x is the state of the controlled plant, $t = N - k$ can be thought of as the number of remaining decision steps, and s can be thought of as the number of remaining jamming instances available to the jammer. We will also say that "x is the state of the plant at stage (s, t)" and write $x_{(s,t)}$ to denote this. We will denote the jammer's action space at stage (s, t) by $\mathcal{A}_{(s,t)} \subseteq \{0, 1\}$.

From an extended state $(x, s, t) \in \mathcal{E}$ such that $\mathcal{A}_{(s,t)} = \{0, 1\}$, the system can transition to two extended states, depending on jammer's and controller's actions at that state: $(Ax+u+w, s, t-1)$ or $(Ax+w, s-1, t-1)$.

The first state is reached when the controller is applying input u and the jammer is inactive ($\alpha = 1$), while the second is reached when the jammer is active ($\alpha = 0$), *regardless of the controller's action*. When $\mathcal{A}_{(s,t)}$ is a strict subset of $\{0, 1\}$, only one of those two transitions is possible. The projection of the extended state space onto the $(s, t)-$ space thus has the structure of the graph of Figure 2.2. In the figure, 'J' denotes that the jammer is active in that stage and 'C' denotes that the jammer is idle (and control signal is received by the plant). Depending on the value of M, some of the depicted transitions may not be possible.

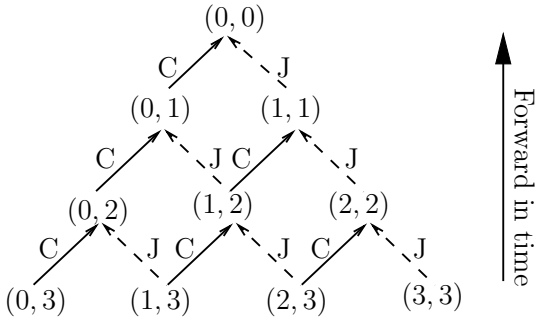


Figure 2.2: A portion of the extended state space.

The original zero-sum dynamic game introduced previously naturally induces a zero-sum dynamic game on the extended state space $\mathcal{E}$ by keeping the same cost function J as in (2.2) and using the extended state transition rule defined above. A controller *feedback* policy on $\mathcal{E}$ is a map $\tilde{\gamma} : \mathcal{E} \to \mathbb{R}$ and, likewise, a jammer feedback policy on $\mathcal{E}$ is a map $\tilde{\mu} : \mathcal{E} \to \{0, 1\}$. Given a controller policy $\tilde{\gamma}$ on $\mathcal{E}$, we can define a feasible policy $\gamma \in \Gamma$ for the original game by

$$\gamma_k(x_{[0,k]}, \alpha_{[0,k-1]}) := \tilde{\gamma}(x_k, M - \text{card}\{i \in [0, k-1] \,|\alpha_i = 0\}, N - k)$$

for all k. Similarly, we can associate a jammer policy $\mu \in \mathcal{M}$ with a feedback jammer policy on $\mathcal{E}$. As a result, if the zero-sum game defined on the extended state space has a saddle-point equilibrium *in feedback strategies*, the original zero-sum game admits a saddle-point equilibrium ($\gamma^* \in \Gamma, \mu^* \in \mathcal{M}$). Note, however, that the converse may not be true, as a feasible strategy γ for the original game does not always uniquely correspond to a feedback strategy $\tilde{\gamma}$ on $\mathcal{E}$ (since, e.g., some γ_k could depend on the exact jamming sequence $\alpha_{[0,k-1]}$ instead of just the number of jamming events so far). As a first approach to the problem of control in the presence of an intelligent jammer, we focus here exclusively on saddle-point equilibrium strategies corresponding to feedback strategies defined on $\mathcal{E}$.

A straightforward generalization of Corollary 6.2 on page 282 of [33], establishes that strategies $\tilde{\gamma}^*$ and $\tilde{\mu}^*$ are feedback saddle-point equilibrium strategies defined on $\mathcal{E}$ if and only if, for all $(s, t) \in \{1, ..., M\} \times \{1, ..., N\}$ there exist functions $V_{(s,t)} : \mathbb{R} \to \mathbb{R}$ such that the following recursive equations hold for all $x \in \mathbb{R}$:

$$V_{(0,0)}(x) = x^2, V_{(s,t)}(x) = \inf_u \max_{\alpha \in \mathcal{A}_{(s,t)}} \left(E\{x^2 + \alpha u^2 + V_{(s^+(\alpha),t-1)}(Ax + \alpha u + w)\} \right). \tag{2.4}$$

In (2.4), we have let $s^+(\alpha) = \begin{cases} s & \text{if } \alpha = 1 \\ s - 1 & \text{if } \alpha = 0 \end{cases}$.

In the next two chapters, we explicitly compute such functions $V_{(s,t)}$, thus effectively and constructively

proving the existence of feedback saddle-point equilibrium strategies defined on $\mathcal{E}$, and, in turn, of saddle-point equilibrium strategies in $\Gamma \times \mathcal{M}$ for the original game with and without state constraints. At this point, it is worth emphasizing that the equality between inf-max and max-inf does indeed hold in (2.4), i.e., that the game has a value. This follows directly from the facts that the function $u \mapsto E\{x^2 + V_{(s-1,t-1)}(Ax+w)\}$ (which appears in the right hand-side of (2.4) when $\alpha = 0$) is a constant and the following lemma.

Lemma 2.1 *Let f be a function and M be a constant. Then* $\inf_u \max(f(u), M) = \max(\inf_u f(u), M)$.

Proof: Let $\mathcal{U} := \{u | f(u) < M\}$. Then we have two cases: $\mathcal{U} = \emptyset$ and $\mathcal{U} \neq \emptyset$. When $\mathcal{U} = \emptyset$,

$$f(u) \geq M \text{ for all } u, \tag{2.5}$$

and hence $\max(f(u), M) = f(u)$ for all u and $\inf_u \max(f(u), M) = \inf_u f(u)$. Besides, inequality (2.5) also implies that $\inf_u f(u) \geq M$, so that $\max(\inf_u f(u), M) = \inf_u f(u)$. Now, if $\mathcal{U} \neq \emptyset$, then $\inf_u f(u) < M$ and $\max(\inf_u f(u), M) = M$. On the other hand, by definition, $\max(f(u), M) \geq M$ for all u and, since $\mathcal{U} \neq \emptyset$, there exists u_0 such that $\max(f(u_0), M) = M$. Hence, $\inf_u \max(f(u), M) = M$. ∎

2.3 Notation

We now introduce some notations. We denote the jammer's and controller's best response costs at stage (s,t), respectively as

$$\begin{aligned}
J_{(s,t)}(x,u,\alpha) &:= E\{x^2 + \alpha u^2 + V_{(s^+(\alpha),t-1)}(Ax + \alpha u + w)\}, \\
J^J_{(s,t)}(x) &:= x^2 + E\{V_{(s-1,t-1)}(Ax+w)\}, \\
\mathscr{J}^C_{(s,t)}(x,u) &:= E\{x^2 + u^2 + V_{(s,t-1)}(Ax + u + w)\} \\
J^C_{(s,t)}(x) &:= \inf_u \mathscr{J}^C_{(s,t)}(x,u) = \inf_u E\{x^2 + u^2 + V_{(s,t-1)}(Ax+u+w)\}.
\end{aligned}$$

With these notations, feedback saddle-point equilibrium strategies defined on $\mathcal{E}$ are characterized by the fact that, when the plant state is x at stage (s,t), the controller's action minimizes $J_{(s,t)}(x,u,\alpha)$ over u, while the jammer is choosing the action corresponding to the largest of the two costs between $J^C_{(s,t)}(x)$ and $J^J_{(s,t)}(x)$ when $\mathcal{A}_{(s,t)} = \{0,1\}$. As we will see, this results in a threshold-based policy in which the action of the jammer at (s,t) depends on the sign of the quantity $|x| - \tau_{(s,t)}(x)$ for an off-line computable threshold function $\tau_{(s,t)}(x)$.

Another object that we will make frequent use of in the next two chapters is the conditional probability density function of the state at a given stage. When a transition from stage (s,t) to stage (s',t') is possible in Figure 2.2, and control action u is applied at stage (s,t), we denote this conditional probability density function of the state $x_{(s',t')}$ given the state $x_{(s,t)}$ and u by $f(x_{(s',t')}|x_{(s,t)},u)$. If the jammer was inactive during the stage (s,t), then $s' = s$, $t' = t-1$, and $x_{(s',t')} = Ax_{(s,t)} + u + w_{N-t}$. Since the noise $\{w_k\}$ is a sequence of i.i.d. Gaussian random variables, the conditional probability density function follows a normal distribution, given by

$$f\left(x_{(s,t-1)} | x_{(s,t)}, u\right) = \mathscr{N}\left(Ax_{(s,t)} + u, \sigma_w^2\right). \tag{2.6}$$

If the jammer is active at stage (s,t), $s' = s-1$, $t' = t-1$, and $x_{(s',t')} = Ax_{(s,t)} + w_{N-t}$ so that the conditional probability density function is

$$f\left(x_{(s-1,t-1)}|x_{(s,t)},u\right) = \mathscr{N}\left(Ax_{(s,t)},\sigma_w^2\right). \tag{2.7}$$

Note that it does not depend on control action u in this case.

Let $\Gamma \in \mathbb{R}^{n\times n}$ be a positive semi-definite matrix, i.e. $\Gamma \geq 0$. Denote two Riccati-type mappings $\mathcal{R}^C(\Gamma)$ and $\mathcal{R}^J(\Gamma)$ on Γ as

$$\mathcal{R}^C(\Gamma) = \left(A^T\Gamma A + Q - A^T\Gamma B(R+B^T\Gamma B)^{-1}B^T\Gamma A\right), \tag{2.8}$$

$$\mathcal{R}^J(\Gamma) = \left(A^T\Gamma A + Q\right). \tag{2.9}$$

For the case with state constraint treated in Chapter 4, we write the cost function as $J^J_{(s,t,\varrho)}$ and $J^C_{(s,t,\varrho)}$ for the case when the jammer is assumed to be active and for the case when the jammer is inactive respectively. This is done to emphasize the fact that the cost functions in this case are dependent on the state constraint ϱ. The value function for the game is denoted by $V_{(s,t,\varrho)}$ at each stage (s,t).

With these notations, we now study jamming attack without state constraint in the next chapter. In Chapter 4, we derive the saddle-point strategy for the zero-sum game under the state constraint.

CHAPTER 3

OPTIMAL CONTROL WITHOUT STATE CONSTRAINTS

Our formulation, detailed in the previous Chapter 2, naturally results in a dynamic zero-sum game between the jammer and the controller. Here, we address the game without state constraints. We show that saddle-point equilibrium strategies exist and use dynamic programming to compute them. In particular, we show that the jammer saddle-point equilibrium strategy is threshold-based, which means that at every time step, the jammer jams if and only if the plant's state is larger than an off-line computable and time-varying threshold. We start by investigating a simple situation in Section 3.1, in which the jammer can only act once over a 3-steps horizon. We derive the threshold functions analytically in this case. The case of general N with $M = 1$ is then treated in Section 3.2. Then, we extend the analysis to the general case of any pair of (M, N), $M < N$ in Section 3.3. We investigate the case of jamming attack on multi-dimensional system in Section 3.4 and discuss challenges in obtaining the solution for this class of games in multi-dimensional system. Finally, we provide numerical simulations in the Section 3.5, which complement the theoretical results obtained in the chapter. Parts of this chapter have been reported in our conference publication [34].

3.1 The $M = 1, N = 3$ case

In order to illustrate the main steps of our derivations while keeping notation to a minimum, we start by computing feedback saddle-point equilibrium strategies $(\tilde{\gamma}^*, \tilde{\mu}^*)$ for the extended game in the simple case where $N = 3$ and $M = 1$ (i.e., the jammer can only jam once in three time steps). By definition, $V_{(0,0)}(x) = x^2$. At the next step, we can be in either of the two stages $(0, 1)$ and $(1, 1)$, depending upon whether the jammer was active in the last decision period or not (see Figure 2.2). At stage $(0, 1)$, the jammer has no chance left to jam and his action space is reduced to $\mathcal{A}_{(0,1)} = \{1\}$. The jammer's best response cost is thus

$$\mathscr{J}^C_{(0,1)}(x, u) = E\{(Ax + u + w_2)^2 + x^2 + u^2\},$$

where expectation is taken over the noise added to the system at this time step. This is a convex function in control u and therefore, first order necessary condition for optimality is also sufficient for the control to be optimal. Using the first order necessary condition for optimality, we find that the optimal control action $\tilde{\gamma}^*(x, 0, 1)$ satisfies

$$\frac{\partial \mathscr{J}^C_{(0,1)}}{\partial u} = 2(Ax + \tilde{\gamma}^*(x, 0, 1)) + 2\tilde{\gamma}^*(x, 0, 1) = 0,$$

i.e., $\tilde{\gamma}^*(x,0,1) = -\frac{A}{2}x$. The value function at this stage is

$$V_{(0,1)}(x) = \left(1 + \frac{A^2}{2}\right) x^2 + \sigma_w^2. \tag{3.1}$$

In stage $(1,1)$, the jammer must always jam, otherwise the jammer constraint is violated. The value function at $(1,1)$ is

$$V_{(1,1)}(x) = J^J_{(1,1)}(x) = (1 + A^2)x^2 + \sigma_w^2. \tag{3.2}$$

Clearly, the value function with control in (3.1) is lower than the expected cost without control in (3.2). Let us now move on to stages $(0,2)$ and $(1,2)$. Note that the noise w_1 in these stages is independent from the noise w_2 occurring in the next stage. Applying the same approach as above, we find that the optimal control for stage $(0,2)$ is

$$\tilde{\gamma}^*(x,0,2) = -A\left(\frac{1 + \frac{A^2}{2}}{2 + \frac{A^2}{2}}\right) x$$

and that the corresponding value function is given by

$$V_{(0,2)}(x) = \left(1 + A^2 - \frac{2A^2}{4 + A^2}\right) x^2 + \left(2 + \frac{A^2}{2}\right) \sigma_w^2.$$

Define $\kappa^{1,C}_{(0,2)} = \left(1 + A^2 - \frac{2A^2}{4+A^2}\right)$ and $\kappa^{2,C}_{(0,2)} = \left(2 + \frac{A^2}{2}\right)$. The case of stage $(1,2)$ requires more effort since the jammer has two options, i.e., $\mathcal{A}_{(1,2)} = \{0,1\}$. At this stage, the two options of the jammer corresponds to - (i) either jam at this stage to reach stage $(0,1)$ and remain idle at the next stage ($t = 1$), or (ii) remain idle at this stage to reach stage $(1,1)$ and jam at the next stage. The controller's best response costs are found to be

$$\begin{aligned}
J^J_{(1,2)}(x) &= \kappa^{1,J}_{(1,2)} x^2 + \kappa^{2,J}_{(1,2)} \sigma_w^2 && (3.3)\\
J^C_{(1,2)}(x) &= \kappa^{1,C}_{(1,2)} x^2 + \kappa^{2,C}_{(1,2)} \sigma_w^2, && (3.4)\\
\text{where } \kappa^{1,J}_{(1,2)} &= 1 + A^2\left(1 + \frac{A^2}{2}\right), \ \ \kappa^{2,J}_{(1,2)} = 2 + \frac{A^2}{2}, && (3.5)\\
\kappa^{1,C}_{(1,2)} &= 1 + A^2 - \frac{A^2}{2 + A^2}, \ \ \kappa^{2,C}_{(1,2)} = 2 + A^2. && (3.6)
\end{aligned}$$

For a given state x, the jammer can enforce the higher of the two costs by choosing to jam if the difference between these costs $J^J_{(1,2)}(x) - J^C_{(1,2)}(x)$ is non-negative and not to jam if the difference is negative. The difference in the cost with jamming and with control is

$$J^J_{(1,2)}(x) - J^C_{(1,2)}(x) = \left(\frac{A^6 + 2A^4 - 2A^2}{2(2 + A^2)}\right) x^2 - \frac{A^2}{2}\sigma_w^2$$

The threshold for this stage is calculated by solving for x such that this difference in cost is greater than

zero i.e. $\{x : J^J_{(1,2)}(x) - J^C_{(1,2)}(x) \geq 0\}$. This yields

$$|x| \quad \geq \quad \sqrt{\left(\frac{2+A^2}{A^4+2A^2+2}\right)}\sigma_w.$$

Define $\tau_{(1,2)} = \sqrt{\left(\frac{2+A^2}{A^4+2A^2+2}\right)}\sigma_w$ to be the threshold for this stage $(1,2)$. In order to increase the cost to the controller, the jammer will jam if the state is above threshold $\tau_{(1,2)}$ as defined in the previous equation. The value at stage $(1,2)$ is

$$V_{(1,2)}(x) = \begin{cases} J^J_{(1,2)}(x) & \text{if } |x| \geq \tau_{(1,2)} \\ J^C_{(1,2)}(x) & \text{if } |x| < \tau_{(1,2)} \end{cases} \tag{3.7}$$

where we defined $\tau_{(1,2)} := \sqrt{\left(\frac{2+A^2}{A^4+2A^2+2}\right)}\sigma_w$. The feedback saddle-point equilibrium strategies $(\tilde{\gamma}^*, \tilde{\mu}^*)$ is

$$\tilde{\mu}^*(x,1,2) = \begin{cases} 0 & \text{if } |x| \geq \tau_{(1,2)} \\ 1 & \text{if } |x| < \tau_{(1,2)} \end{cases},$$
$$\text{and } \tilde{\gamma}^*(x,1,2) = -A\left(\frac{1+A^2}{2+A^2}\right)x \quad \forall\, x.$$

It can be observed that the value function $V_{(1,2)}$ is an even and convex function of state x, since it is maximum of two convex functions $J^J_{(1,2)}$ and $J^C_{(1,2)}$. We will make use of this fact in proving the convexity of value function in the next stage.

Let us now consider stage $(1,3)$, the initial stage. The controller's cost if the jammer decides to jam at this stage is

$$J^J_{(1,3)}(x) = \kappa^{1,J}_{(1,3)}x^2 + \kappa^{2,J}_{(1,3)}\sigma_w^2$$
$$\text{where } \kappa^{1,J}_{(1,3)} = \left(1 + A^2\kappa^{1,C}_{(0,2)}\right),\ \kappa^{2,J}_{(1,3)} = \kappa^{1,C}_{(0,2)} + \kappa^{2,C}_{(0,2)}$$

If the jammer chooses not to jam at stage $(1,3)$, then the controller incurs a cost $\mathscr{J}^C_{(1,3)}(x,u)$. In one case, the state in the next stage $(1,2)$ can fall into the region $|x_1| \geq \tau_{(1,2)}$. This means that the jammer will choose to jam at that stage. Second case is that the state falls into the region $|x_1| < \tau_{(1,2)}$ and the jammer will jam at a later step. We need to analyze the cost to the controller in both the cases separately. The conditional probability of x_1 given x_0 is $f(x_1|x) = \mathscr{N}(Ax+u, \sigma_w^2)$. To compute the controller's best response cost when the jammer is idle, $J^C_{(1,3)}$, we need to calculate $E(V_{(1,2)}(x_1))$, where $x_1 = Ax + u + w$ for a given controller action u. According to (3.7), and recalling the definition of $f(.|.)$ introduced in Section 2.3, we see that

$$E(V_{(1,2)}(x_1)) = \int_{|x_1|\geq\tau_{1,2}} f(x_1|x,u)J^J_{(1,2)}(x_1)dx_1 + \int_{|x_1|<\tau_{1,2}} f(x_1|x,u)J^C_{(1,2)}(x_1)dx_1. \tag{3.8}$$

Let us introduce $P_{(1,3)}(x,u)$ as the conditional probability that $|x_{(1,2)}|$ lies above the threshold $\tau_{1,2}$, given

that the state at stage $(1,3)$ is x and the control action at stage $(1,3)$ is u,

$$P_{(1,3)}(x,u) \;=\; \int_{|x_1|\geq\tau_{(1,2)}} f(x_1|x,u)dx_1. \tag{3.9}$$

Let us also write $\overline{P}_{(1,3)}(x,u) = 1 - P_{(1,3)}(x,u)$ for the conditional probability that $|x_{(1,2)}| < \tau_{(1,2)}$, and introduce the following two second moments of x_1

$$R_{(1,3)}(x,u) = \frac{\int_{|x_1|\geq\tau_{(1,2)}} x_1^2 f(x_1|x,u)dx_1}{(Ax+u)^2+\sigma_w^2} \tag{3.10}$$

and $\overline{R}_{(1,3)}(x,u) := 1 - R_{(1,3)}(x,u)$. The cost at stage $(1,3)$ with control is

$$\mathscr{J}^C_{(1,3)}(x,u) = x^2 + u^2 + E(V_{(1,2)}(Ax+u+w_0)|x). \tag{3.11}$$

Using the notation introduced above, the cost at stage $(1,3)$ is given by

$$\begin{aligned}\mathscr{J}^C_{(1,3)}(x,u) \;=\;& x^2+u^2+(Ax+u)^2\left(R_{(1,3)}\kappa^{1,J}_{(1,2)}+\overline{R}_{(1,3)}\kappa^{1,C}_{(1,2)}\right)+\sigma_w^2\left(R_{(1,3)}\kappa^{1,J}_{(1,2)}+\overline{R}_{(1,3)}\kappa^{1,C}_{(1,2)}\right.\\ &\left.+P_{(1,3)}\kappa^{2,J}_{(1,2)}+\overline{P}_{(1,3)}\kappa^{2,C}_{(1,2)}\right).\end{aligned} \tag{3.12}$$

Next, we state a proposition, which proves that the cost function is convex in state and control variables.

Proposition 3.1 *Let h be a (strictly) convex function and w be a random variable. Then $x \mapsto E_w\{h(x+w)\}$ is a (strictly) convex function in x, where $E_w\{\cdot\}$ denotes the expectation with respect to the random variable w.*

Proof: Since $h(x)$ is convex, we have

$$h(\lambda x_1 + (1-\lambda)x_2) \leq \lambda h(x_1) + (1-\lambda)h(x_2).$$

Therefore, using this inequality in the expression for the expectation, we get

$$\begin{aligned}E_w\{h(\lambda x_1+(1-\lambda)x_2+w)\} \;&\leq\; E_w\{\lambda h(x_1+w)+(1-\lambda)h(x_2+w)\},\\ &=\; \lambda E_w\{h(x_1+w)\}+(1-\lambda)E_w\{h(x_2+w)\}.\end{aligned}$$

Here, the first inequality follows from the definition of convex function and positivity of probability distribution of random variable w. Hence, if the random variable is added linearly to the state, then the expectation value of a convex function is also be a convex function. The proof for strictly convex case is the same with strict inequality in the first relationship above. ∎

From the proposition above, we know that the cost function in (3.11) is convex in control u. Therefore, first order necessary condition for optimality is also sufficient for obtaining the optimal control $\tilde{\gamma}^*(x,1,3)$. To

obtain the optimal control, we differentiate the cost function in (3.11) with respect to u to get

$$\frac{d\mathscr{J}^C_{(1,3)}}{du} = H(x,u) := 2u + 2(Ax+u)\left(R_{(1,3)}\kappa^{1,J}_{(1,2)} + \overline{R}_{(1,3)}\kappa^{1,C}_{(1,2)}\right) + \left((Ax+u)^2 + \sigma_w^2\right) \left(\kappa^{1,J}_{(1,2)} - \kappa^{1,C}_{(1,2)}\right)\frac{dR_{(1,3)}}{du} + \sigma_w^2\left(\kappa^{2,J}_{(1,2)} - \kappa^{2,C}_{(1,2)}\right)\frac{dP_{(1,3)}}{du}, \tag{3.13}$$

and set it equal to zero. This gives an implicit equation $H(x,u)=0$ characterizing $\tilde{\gamma}^*(x,1,3)$. Now, letting $L_{(1,3)}(x) := -\tilde{\gamma}^*(x,1,3)/(Ax)$ and plugging the obtained value of $\tilde{\gamma}^*(x,1,3)$ back into (3.11), yields

$$J^C_{(1,3)}(x) = \kappa^{1,C}_{(1,3)}(x)x^2 + \kappa^{2,C}_{(1,3)}(x)\sigma_w^2 \tag{3.14}$$

where $P_{(1,3)} := P_{(1,3)}(x,\tilde{\gamma}^*(x,1,3))$, $R_{(1,3)} := R_{(1,3)}(x,\tilde{\gamma}^*(x,1,3))$ and

$$\kappa^{1,C}_{(1,3)}(x) = 1 + A^2L^2_{(1,3)}(x) + A^2(1-L_{(1,3)}(x))^2\left(R_{(1,3)}\kappa^{1,J}_{(1,2)} + \overline{R}_{(1,3)}\kappa^{1,C}_{(1,2)}\right), \tag{3.15}$$

$$\kappa^{2,C}_{(1,3)}(x) = \left(R_{(1,3)}\kappa^{1,J}_{(1,2)} + \overline{R}_{(1,3)}\kappa^{1,C}_{(1,2)} + P_{(1,3)}\kappa^{2,J}_{(1,2)} + \overline{P}_{(1,3)}\kappa^{2,C}_{(1,2)}\right). \tag{3.16}$$

Once both functions $J^J_{(1,3)}(x)$ and $J^C_{(1,3)}(x)$ have been determined, the value function at stage $(1,3)$ is

$$V_{(1,3)}(x) = \begin{cases} J^J_{(1,3)}(x) & \text{if } |x| \geq \tau_{(1,3)}(x) \\ J^C_{(1,3)}(x) & \text{if } |x| < \tau_{(1,3)}(x) \end{cases}, \tag{3.17}$$

where the threshold function $\tau_{(1,3)}(x)$ is defined such that $J^J_{(1,3)}(x) - J^C_{(1,3)}(x) \geq 0$ if and only if $|x| \geq \tau_{(1,3)}(x)$. Analytically, we find that

$$\tau_{(1,3)}(x) = \sqrt{\frac{\kappa^{2,C}_{(1,3)}(x) - \kappa^{2,J}_{(1,3)}}{\kappa^{1,J}_{(1,3)} - \kappa^{1,C}_{(1,3)}(x)}}\sigma_w. \tag{3.18}$$

Note that, unlike $\tau_{(1,2)}$, threshold function $\tau_{(1,3)}$ is not constant, and that its computation requires determining $\tilde{\gamma}(.,1,3)$. Also note that $\kappa^{1,C}_{(1,3)}(x)$ and $\kappa^{2,C}_{(1,3)}(x)$ are even functions, i.e., that $\kappa^{1,C}_{(1,3)}(-x) = \kappa^{1,C}_{(1,3)}(x)$ and $\kappa^{2,C}_{(1,3)}(-x) = \kappa^{2,C}_{(1,3)}(x)$. This is because $P_{(1,3)}(-x,-u) = P_{(1,3)}(x,u)$ and the same property holds for $R_{(1,3)}(x,u)$. As a result, $\tau_{(1,3)}(x)$ is even.

We will make use of the following proposition to prove that the value function in (3.17) is a convex function of state.

Proposition 3.2 *Let h be a non-negative convex function in $(x,u) \in \mathbb{R}\times\mathbb{R}$. Then $H(x) := \inf_u h(x,u)$ is a convex function in x.*

Proof: For proof, the reader is referred to [35], pp 102. ∎

Letting $h = \mathscr{J}^C_{(1,3)}$ in the proposition above, we find that the optimal cost with control $J^C_{(1,3)}$ is a convex function of state x. Again, the value function in (3.17) is the maximum of two convex functions, and is therefore, a convex function.

We are now in a position to prove two results, which give us an insight into the nature of threshold function $\tau_{(1,3)}$. In the next lemma, we prove that the control policy can never be a deadbeat policy. Then we make use of this fact to prove that the threshold function has a limit as the state tends to infinity.

Lemma 3.3 $L_{(1,3)}(x) \neq 1 \; \forall \; x \neq 0$.

Proof: We prove this by contradiction. If $L_{(1,3)}(x) = 1$, then the optimal control $u^*(x) = -Ax$ and (3.13) vanishes at $u = -Ax$. Therefore, it is sufficient to prove that (3.13) doesn't vanish at $u = -Ax$. Consider the derivative of $R_{(1,3)}(x,u)$ and $P_{(1,3)}(x,u)$ with respect to u.

$$\frac{dR_{(1,3)}(x,u)}{du} = \int_{|x_1| \geq \tau_{(1,2)}} x_1^2 \exp\left(-\frac{(x_1-(Ax+u))^2}{2\sigma_w^2}\right) \frac{\left(\frac{x_1-(Ax+u)}{\sigma_w^2} - \frac{2(Ax+u)}{(Ax+u)^2+\sigma_w^2}\right)}{(Ax+u)^2+\sigma_w^2} dx_1 \quad (3.19)$$

$$\frac{dP_{(1,3)}(x,u)}{du} = \int_{|x_1| \geq \tau_{(1,2)}} \frac{(x_1-(Ax+u))}{\sigma_w^2} \exp\left(-\frac{(x_1-(Ax+u))^2}{2\sigma_w^2}\right) dx_1 \quad (3.20)$$

If we put $u = -Ax$ in (3.19) and (3.20), the function being integrated becomes odd and the interval in which it is being integrated is $(-\infty, -\tau_{(1,2)}) \cup (\tau_{(1,2)}, \infty)$. Thus, they vanish at $u = -Ax$. Using this relation in (3.13) for $x \neq 0$, we get

$$\left.\frac{d\mathscr{J}^C_{(1,3)}}{du}\right|_{u=-Ax} = 2u = -2Ax \neq 0 \quad (3.21)$$

Therefore, the optimal control $u^*(x)$ can never be equal to $-Ax$. This proves $L_{(1,3)}(x) = -u^*(x)/(Ax) \neq 1$ and the optimal control strategy can never be deadbeat. ■

Proposition 3.4 *As the state x tends to infinity, $\lim_{|x|\to\infty} \tau_{(1,3)}(x)$ exists.*

Proof: From Lemma 3.3, we know that $L_{(1,3)}(x) \neq 1 \; \forall \; x \neq 0$. Define $u^*(x) := \tilde{\gamma}^*(x,1,3) \neq -Ax$. Therefore, as state $|x| \to \infty$, $|Ax + u^*(x)| \to \infty$ also holds. We are interested in limiting value of $L_{(1,3)}(x)$. Taking the limit $|x| \to \infty$ in (3.9) and (3.10), we get

$$\lim_{|x|\to\infty} P_{(1,3)}(x,u^*(x)) = 1, \qquad \lim_{|x|\to\infty} \overline{P}_{(1,3)}(x,u^*(x)) = 0$$
$$\lim_{|x|\to\infty} R_{(1,3)}(x,u^*(x)) = 1, \qquad \lim_{|x|\to\infty} \overline{R}_{(1,3)}(x,u^*(x)) = 0$$

Also, derivative of $P_{(1,3)}(x,u^*(x))$ in (3.20) vanish as $|x| \to \infty$. The derivative term of $R_{(1,3)}(x,u^*(x))$ in (3.13) in the limit is

$$\lim_{|x|\to\infty} \left((Ax+u)^2+\sigma_w^2\right) \left.\frac{dR_{(1,3)}(x,u)}{du}\right|_{u=u^*(x)} = 0$$

If we divide (3.13) by Ax at optimal control $u^*(x)$, it still remains 0. Using these relations, we get

$$\lim_{|x|\to\infty} \frac{1}{Ax} \left.\frac{d\mathscr{J}^C_{(1,3)}}{du}\right|_{u=u^*(x)} = 0$$

which simplifies to

$$\lim_{|x|\to\infty} -2L_{(1,3)}(x) + 2(1-L_{(1,3)}(x))\kappa^{1,J}_{(1,2)} = 0$$

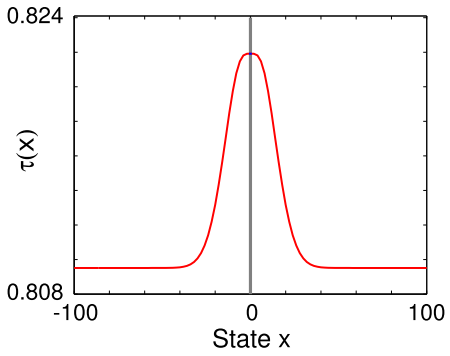


Figure 3.1: Graph of function $\tau_{(1,3)}(x)$ for $A = 2.5$ and $\sigma_w = 1$.

This relation yields

$$\lim_{|x|\to\infty} L_{(1,3)}(x) = \frac{\kappa^{1,J}_{(1,2)}}{1+\kappa^{1,J}_{(1,2)}} \tag{3.22}$$

Putting this limiting value of $L_{(1,3)}$ in (3.15) and (3.16), we get

$$\lim_{|x|\to\infty} \kappa^{1,C}_{(1,3)}(x) = 1 + A^2 \frac{\kappa^{1,J}_{(1,2)}}{1+\kappa^{1,J}_{(1,2)}} \tag{3.23}$$

$$\lim_{|x|\to\infty} \kappa^{2,C}_{(1,3)}(x) = \kappa^{1,J}_{(1,2)} + \kappa^{2,J}_{(1,2)} \tag{3.24}$$

Taking the limit in (3.18) and substituting (3.23) and (3.24),

$$\lim_{|x|\to\infty} \tau_{(1,3)}(x) = \sqrt{\frac{\kappa^{1,J}_{(1,2)} + \kappa^{2,J}_{(1,2)} - \kappa^{2,J}_{(1,3)}}{\kappa^{1,J}_{(1,3)} - (1 + A^2 \frac{\kappa^{1,J}_{(1,2)}}{1+\kappa^{1,J}_{(1,2)}})}}\sigma_w \tag{3.25}$$

which proves the lemma. ■

Figure 3.1 shows the graph of the threshold function $\tau_{(1,3)}(x)$. As predicted by Lemma 3.4, we observe that the threshold $\tau_{(1,3)}(x)$ reaches the limiting value given by (3.25) when the state value x is sufficiently large. Also notice that when the state is sufficiently large, the value of $|x| - \tau_{(1,3)}(x)$ is greater than 0, and it is beneficial for jammer to jam in this region. In the dark-colored narrow strip, absolute value of state $|x|$ is less than the threshold $\tau_{(1,3)}(x)$, while the reversed inequality holds in the white region. The jammer is active at stage $(1,3)$ if x belongs to the white region.

3.2 A General Case with $M = 1$

Before we compute the optimal strategies for the controller and the jammer, let us first prove the following theorem.

Theorem 3.5 *The value function $V_{(s,t)}$ at all stages (s,t) is strictly convex in state x for all $0 \le s \le t$.*

Proof: This statement can be proved using induction on t and then by induction on s. The base case is stage $(0,0)$, at which the value function is $V_{(0,0)}(x) = x^2$, which is a strictly convex function of state. Using optimal control theory, we know that at each stage $(0,t),\ t \geq 1$, the value function is quadratic in state (see Theorem 3.7). Hence, the value function $V_{(0,t)}$ is strictly convex function of state. We also know that the value functions at stage (t,t) is strictly convex (and in fact, quadratic in state x). In the previous section, we showed that the value function is strictly convex in state at stage $(1,2)$. Let us assume that the value function is strictly convex at stage $(1,t)$. Then at stage $(1,t+1)$, the cost functions are

$$\begin{aligned} J^J_{(1,t+1)}(x) &= E\{x^2 + V_{(0,t)}(Ax+w)\}, \\ J^C_{(1,t+1)}(x) &= \inf_u E\{x^2 + u^2 + V_{(1,t)}(Ax+u+w)\}. \end{aligned}$$

By Propositions 3.1 and 3.2, the cost functions are strictly convex functions of state. The value function

$$V_{(1,t+1)}(x) = \max\{J^J_{(1,t+1)}(x), J^C_{(1,t+1)}(x)\}$$

is the maximum of these two cost functions. Hence, the value function $V_{(1,t+1)}$ is a strictly convex function. Hence for a fixed t, all the value functions are strictly convex in state for all values of $s \leq t$. Similar to the steps above, we can prove that the value function $V_{(s+1,t+1)}$ is convex if the value functions $V_{(s,t)}$ and $V_{(s+1,t)}$ is convex. This completes the induction step and we get the proof of the statement. ∎

Next, we have following lemma which shows that as a result of Theorem 3.5 proved above, we also have a unique control action at each decision step.

Lemma 3.6 *The optimal control at each stage (s,t) exists and is unique.*

Proof: Using Proposition 3.1 and Theorem 3.5, we can infer that the cost function is strictly convex in the control. Also, we have following observation

$$\lim_{|u_{(s,t)}| \to \infty} \mathscr{J}^C_{(s,t)}(x_{(s,t)}, u_{(s,t)}) = \infty.$$

Then, there is a unique control value which minimizes the cost. Therefore, the first order necessary condition for optimality is also sufficient in this case. ∎

Now, building on the intuition drawn from the results of Section 3.1, we can prove the following theorem regarding the existence and characterization of feedback saddle-point equilibrium strategies defined on $\mathcal{E}$ in the case where $M = 1$ and N is arbitrary. The result is proved by induction on t.

Theorem 3.7 *Let $M = 1$ and $N > 1$. Let the coefficients be defined according to the following recursion:*

$$\begin{aligned} \kappa^{1,C}_{(0,0)} &= 1, & \kappa^{2,C}_{(0,0)} &= 0, \\ \kappa^{1,C}_{(0,t)} &= 1 + A^2 \tfrac{\kappa^{1,C}_{(0,t-1)}}{1+\kappa^{1,C}_{(0,t-1)}}, & \kappa^{2,C}_{(0,t)} &= \kappa^{1,C}_{(0,t-1)} + \kappa^{2,C}_{(0,t-1)}, \\ \kappa^{1,J}_{(1,t)} &= 1 + A^2 \kappa^{1,C}_{(0,t-1)}, & \kappa^{2,J}_{(1,t)} &= \kappa^{1,C}_{(0,t-1)} + \kappa^{2,C}_{(0,t-1)}, \\ \kappa^{1,C}_{(1,t)}(x) &= 1 + A^2 \left(L^2_{(1,t)}(x) + (1 - L_{(1,t)}(x))^2 \psi^1_{(1,t)}(x, \tilde{\gamma}^*(x,1,t)) \right), \\ \kappa^{2,C}_{(1,t)}(x) &= \psi^1_{(1,t)}(x, \tilde{\gamma}^*(x,1,t)) + \psi^2_{(1,t)}(x, \tilde{\gamma}^*(x,1,t)), \end{aligned}$$

for all $t \geq 1$ and all x, where, the set $\mathcal{X}_{(1,t)}$ is defined as

$$\mathcal{X}_{(1,t)} = \left\{ x_{(1,t)} \in \mathbb{R} : x_{(1,t)}^2 - \tau_{(1,t)}^2(x_{(1,t)}) \geq 0 \right\},$$

the threshold $\tau_{(1,t)}(x_{(1,t)})$ and $\psi(x,u)$'s are defined as

$$\begin{aligned}
\tau_{(1,t)}(x_{(1,t)}) &= \sqrt{\frac{\kappa_{(1,t)}^{2,C}(x_{(1,t)}) - \kappa_{(1,t)}^{2,J}}{\kappa_{(1,t)}^{1,J} - \kappa_{(1,t)}^{1,C}(x_{(1,t)})}}\sigma_w, \\
\psi_{(1,t)}^1(x,u) &= \int_{\mathcal{X}_{(1,t-1)}^c} \frac{\kappa_{(1,t-1)}^{1,C}(\bar{x})\bar{x}^2}{(Ax+u)^2+\sigma_w^2} f(\bar{x}|x,u)d\bar{x} + R_{(1,t)}(x,u)\kappa_{(1,t-1)}^{1,J} \\
\psi_{(1,t)}^2(x,u) &= \int_{\mathcal{X}_{(1,t-1)}^c} \kappa_{(1,t-1)}^{2,C}(\bar{x}) f(\bar{x}|x,u)d\bar{x} + P_{(1,t)}(x,u)\kappa_{(1,t-1)}^{2,J},
\end{aligned}$$

conditional probability and second moment defined as

$$\begin{aligned}
P_{(1,t)}(x_{(1,t)}, u_{(1,t)}) &= Pr\left\{ x_{(1,t-1)} \in \mathcal{X}_{(1,t-1)} | x_{(1,t)}, u_{(1,t)} \right\}, \\
R_{(1,t)}(x_{(1,t)}, u_{(1,t)}) &= \frac{\int_{\mathcal{X}_{(1,t-1)}} x^2 f(x|x_{(1,t)}, u_{(1,t)})dx}{(Ax_{(1,t)} + u_{(1,t)})^2 + \sigma_w^2},
\end{aligned}$$

and optimal control $\tilde{\gamma}^*(x,1,t)$ is

$$\tilde{\gamma}^*(x,1,t) = \arg\inf_u \left[x^2 + u^2 + (Ax+u)^2\psi_{(1,t)}^1(x,u) + \sigma_w^2 \left(\psi_{(1,t)}^1(x,u) + \psi_{(1,t)}^2(x,u) \right) \right].$$

Then, the strategies $(\tilde{\gamma}^*, \tilde{\mu}^*)$ given below are feedback saddle-point equilibrium strategies defined on $\mathcal{E}$:

$$\begin{aligned}
\tilde{\gamma}^*(x,0,t) &= -\left(\frac{A\kappa_{(0,t-1)}^{1,C}}{1+\kappa_{(0,t-1)}^{1,C}} \right) x; \qquad \tilde{\mu}^*(x,0,t) = 1 \; \forall \, t,x, \\
\tilde{\mu}^*(x,1,t) &= \begin{cases} 0 & \text{if } x \in \mathcal{X}_{(1,t)} \\ 1 & \text{if } x \in \mathcal{X}_{(1,t)}^c \end{cases}
\end{aligned}$$

and $\tilde{\gamma}^*(x,1,t)$ as obtained above.

Proof: This theorem can be proved using induction. As shown in the Section 3.1, the theorem holds for the base case of induction, i.e. for stage $(0,0)$, $(0,1)$ and $(1,1)$. We denote the cost function of the game at stage $(1,t-1)$ as

$$\begin{aligned}
J_{(1,t-1)}^J(x_{(1,t-1)}) &= \kappa_{(1,t-1)}^{1,J} x_{(1,t-1)}^2 + \kappa_{(1,t-1)}^{2,J}\sigma_w^2, \\
J_{(1,t-1)}^C(x_{(1,t-1)}) &= \kappa_{(1,t-1)}^{1,C}(x_{(1,t-1)}) x_{(1,t-1)}^2 + \kappa_{(1,t-1)}^{2,C}(x_{(1,t-1)})\sigma_w^2,
\end{aligned}$$

with the value function as

$$V_{(1,t-1)}(x_{(0,t-1)}) = \max\left\{ J_{(1,t-1)}^J(x_{(1,t-1)}), J_{(1,t-1)}^C(x_{(1,t-1)}) \right\}.$$

At stage $(0, t-1)$, the value of the game is denoted by

$$V_{(0,t-1)}(x_{(0,t-1)}) = \kappa^{1,C}_{(0,t-1)} x^2_{(0,t-1)} + \kappa^{2,C}_{(0,t-1)} \sigma^2_w,$$

where $\kappa^{1,J}_{(1,t-1)}$, $\kappa^{2,J}_{(1,t-1)}$, $\kappa^{1,C}_{(0,t-1)}$ and $\kappa^{2,C}_{(0,t-1)}$ are known constants at step $t-1$ and $\kappa^{1,C}_{(1,t-1)}(x_{(1,t-1)})$ and $\kappa^{2,C}_{(1,t-1)}(x_{(1,t-1)})$ are nonlinear functions of the state at that stage. Now, we derive the coefficients for the value of the game at the next stage, in terms of these quantities.
Consider stage $(0, t)$, where the jammer has 0 chances left to jam and t time steps left to go. The next stage is $(0, t-1)$. The cost in this case is

$$\mathscr{J}^C_{(0,t)}(x_{(0,t)}, u_{(0,t)}) = E\left\{\kappa^{1,C}_{(0,t-1)}(Ax_{(0,t)} + u_{(0,t)} + w_{(0,t)})^2 + \kappa^{2,C}_{(0,t-1)}\sigma^2_w\right\} + x^2_{(0,t)} + u^2_{(0,t)},$$

where the actuation noise $w_{(0,t)}$ is independent of state and previous noise. Rewriting the equation after expansion:

$$\begin{aligned}\mathscr{J}^C_{(0,t)}(x_{(0,t)}, u_{(0,t)}) &= (1 + A^2\kappa^{1,C}_{(0,t-1)})x^2_{(0,t)} + (1 + \kappa^{1,C}_{(0,t-1)})u^2_{(0,t)} + 2A\kappa^{1,C}_{(0,t-1)}x_{(0,t)}u_{(0,t)} \\ &\quad + \left(\kappa^{1,C}_{(0,t-1)} + \kappa^{2,C}_{(0,t-1)}\right)\sigma^2_w. \end{aligned} \tag{3.26}$$

We differentiate the cost with respect to $u_{(0,t)}$ and set it equal to zero to get the optimal control $\tilde{\gamma}^*(x, 0, t)$:

$$\begin{aligned}\frac{d\mathscr{J}^C_{(0,t)}}{du_{(0,t)}} &= 2(1 + \kappa^{1,C}_{(0,t-1)})u_{(0,t)} + 2A\kappa^{1,C}_{(0,t-1)}x_{(0,t)}, \\ \tilde{\gamma}^*(x, 0, t) &= -A\left(\frac{\kappa^{1,C}_{(0,t-1)}}{1 + \kappa^{1,C}_{(0,t-1)}}\right)x_{(0,t)}.\end{aligned}$$

Putting this value of optimal control in (3.26), the value of the game $V^C_{(0,t)}$ is

$$\begin{aligned}J^C_{(0,t)}(x_{(0,t)}) &= \kappa^{1,C}_{(0,t)}x^2_{(0,t)} + \kappa^{2,C}_{(0,t)}\sigma^2_w, \\ \text{where } \kappa^{1,C}_{(0,t)} &= 1 + A^2\frac{\kappa^{1,C}_{(0,t-1)}}{1 + \kappa^{1,C}_{(0,t-1)}}, \\ \kappa^{2,C}_{(0,t)} &= \kappa^{1,C}_{(0,t-1)} + \kappa^{2,C}_{(0,t-1)}.\end{aligned}$$

At stage $(1, t)$, the jammer can choose to jam. The cost with jamming in this case is

$$J^J_{(1,t)} = E\left\{\kappa^{1,C}_{(0,t-1)}(Ax_{(1,t)} + w_{(1,t)})^2 + \kappa^{2,C}_{(0,t-1)}\sigma^2_w\right\} + x^2_{(1,t)},$$

which upon simplification yields

$$\begin{aligned}\kappa^{1,J}_{(1,t)} &= 1 + A^2\kappa^{1,C}_{(0,t-1)}, \\ \kappa^{2,J}_{(1,t)} &= \kappa^{1,C}_{(0,t-1)} + \kappa^{2,C}_{(0,t-1)}.\end{aligned}$$

If the jammer chooses not to jam at stage $(1,t)$, then there would be two cases. The jammer may choose to jam at the next stage $(1,t-1)$ or not jam, depending upon the threshold $\tau_{(1,t-1)}(x_{(1,t-1)})$ at that stage. Notice that the threshold is a function of state $x_{(1,t-1)}$ at next stage. Therefore, the cost at this stage $\mathscr{J}^C_{(1,t)}$ consists of a cost of state and control at this stage, and the expected cost for both the cases conditioned on the state $x_{(1,t)}$ at this stage :

$$\mathscr{J}^C_{(1,t)}(x_{(1,t)},u_{(1,t)}) \quad = \quad x^2_{(1,t)}+u^2_{(1,t)}+E\left\{V_{(1,t-1)}(x_{(1,t-1)})|x_{(1,t)},u_{(1,t)}\right\}.$$

Let $\mathcal{X}_{(1,t-1)}$ denote the set of all states in stage $(1,t-1)$, in which jamming is the cost maximizing strategy for the jammer :

$$\mathcal{X}_{(1,t-1)} \quad = \quad \left\{x_{(1,t-1)}\in\mathbb{R} : x^2_{(1,t-1)}-\tau^2_{(1,t-1)}(x_{(1,t-1)})\geq 0\right\}. \tag{3.27}$$

The probability $P_{(1,t)}$ is the probability that the state $x_{(1,t-1)}$ falls in the set $\mathcal{X}_{(1,t-1)}$ conditioned on the information about the current state $x_{(1,t)}$ i.e.

$$P_{(1,t)}(x_{(1,t)},u_{(1,t)})=\mathbb{P}\{x_{(1,t-1)}\in\mathcal{X}_{(1,t-1)}|x_{(1,t)},u_{(1,t)}\}. \tag{3.28}$$

Similarly, define $R_{(1,t)}(x_{(1,t)},u_{(1,t)})$ as the second moment of the state $x_{(1,t-1)}\in\mathcal{X}_{(1,t-1)}$ conditioned on the state $x_{(1,t)}$:

$$R_{(1,t)}(x_{(1,t)},u_{(1,t)})=\frac{\int_{\mathcal{X}_{(1,t-1)}}x^2_{(1,t-1)}f(x_{(1,t-1)}|x_{(1,t)},u_{(1,t)})dx_{(1,t-1)}}{(Ax_{(1,t)}+u_{(1,t)})^2+\sigma^2_w}. \tag{3.29}$$

Let us define $\psi^1_{(1,t)}(x_{(1,t)},u_{(1,t)})$ and $\psi^2_{(1,t)}(x_{(1,t)},u_{(1,t)})$ as follows :

$$\begin{aligned}\psi^1_{(1,t)}(x_{(1,t)},u_{(1,t)}) \quad &= \quad \int_{\mathcal{X}^c_{(1,t-1)}}\frac{\kappa^{1,C}_{(1,t-1)}(x_{(1,t-1)})x^2_{(1,t-1)}}{(Ax_{(1,t)}+u_{(1,t)})^2+\sigma^2_w}f(x_{(1,t-1)}|x_{(1,t)},u_{(1,t)})dx_{(1,t-1)}\\ &\quad +R_{(1,t)}(x_{(1,t)},u_{(1,t)})\kappa^{1,J}_{(1,t-1)}, \qquad (3.30)\\ \psi^2_{(1,t)}(x_{(1,t)},u_{(1,t)}) \quad &= \quad \int_{\mathcal{X}^c_{(1,t-1)}}\kappa^{2,C}_{(1,t-1)}(x_{(1,t-1)})f(x_{(1,t-1)}|x_{(1,t)},u_{(1,t)})dx_{(1,t-1)}\\ &\quad +P_{(1,t)}(x_{(1,t)},u_{(1,t)})\kappa^{2,J}_{(1,t-1)}. \qquad (3.31)\end{aligned}$$

Notice that the integral is taken over the set $\mathcal{X}^c_{(1,t-1)}$, which is the complementary set of $\mathcal{X}_{(1,t-1)}$ in $\mathbb{R}$, $\mathcal{X}^c_{(1,t-1)}=\mathbb{R}\backslash\mathcal{X}_{(1,t-1)}$. The cost to the controller is given by

$$\begin{aligned}\mathscr{J}^C_{(1,t)}(x_{(1,t)},u_{(1,t)}) \quad &= \quad x^2_{(1,t)}+u^2_{(1,t)}+\left(Ax_{(1,t)}+u_{(1,t)}\right)^2\psi^1_{(1,t)}(x_{(1,t)},u_{(1,t)})\\ &\quad +\sigma^2_w\left(\psi^1_{(1,t)}(x_{(1,t)},u_{(1,t)})+\psi^2_{(1,t)}(x_{(1,t)},u_{(1,t)})\right).\end{aligned}$$

Using Proposition 3.1 and Theorem 3.5, we know that the cost function $\mathscr{J}^C_{(1,t)}$ is a strictly convex function of control $u_{(1,t)}$. Hence, first order necessary condition is also sufficient for optimality of control action.

Differentiating it with respect to $u_{(1,t)}$, we get

$$\frac{d\mathscr{J}^C_{(1,t)}}{du_{(1,t)}} = 2u_{(1,t)} + 2\left(Ax_{(1,t)} + u_{(1,t)}\right)\psi^1_{(1,t)} + \left(Ax_{(1,t)} + u_{(1,t)}\right)^2 \frac{d\psi^1_{(1,t)}}{du_{(1,t)}} + \sigma_w^2\left(\frac{d\psi^1_{(1,t)}}{du_{(1,t)}} + \frac{d\psi^2_{(1,t)}}{du_{(1,t)}}\right), \quad (3.32)$$

which vanish at the optimal value of control $\tilde{\gamma}^*(x,1,t)$

$$\frac{d\mathscr{J}^C_{(1,t)}}{du_{(1,t)}}\left(x, \tilde{\gamma}^*(x,1,t)\right) \quad = \quad 0.$$

This way, we get the optimal control as a function of the state at this stage. Again, define $L_{(1,t)}(x_{(1,t)}) = -\tilde{\gamma}^*(x,1,t)(x_{(1,t)})/(Ax_{(1,t)})$. Then the coefficient for the optimal cost at stage $(1,t)$ if the jammer chooses not to jam is given by

$$\kappa^{1,C}_{(1,t)}(x_{(1,t)}) \quad = \quad 1 + A^2\left(L^2_{(1,t)}(x_{(1,t)}) + (1 - L_{(1,t)}(x_{(1,t)}))^2\psi^1_{(1,t)}(x_{(1,t)})\right), \quad (3.33)$$

$$\kappa^{2,C}_{(1,t)}(x_{(1,t)}) \quad = \quad \psi^1_{(1,t)}(x_{(1,t)}) + \psi^2_{(1,t)}(x_{(1,t)}). \quad (3.34)$$

The threshold at this stage is given by

$$\tau_{(1,t)}(x_{(1,t)}) = \sqrt{\frac{\kappa^{2,C}_{(1,t)}(x_{(1,t)}) - \kappa^{2,J}_{(1,t)}}{\kappa^{1,J}_{(1,t)} - \kappa^{1,C}_{(1,t)}(x_{(1,t)})}}\sigma_w. \quad (3.35)$$

Again, we can compute the set

$$\mathcal{X}_{(1,t)} = \left\{x_{(1,t)} : x^2_{(1,t)} - \tau^2_{(1,t)}(x_{(1,t)}) \geq 0\right\},$$

where the optimal expected cost with jamming is more than the optimal expected cost with control. As we go down the steps, we compute the thresholds at stage $(1,t)$ as a function of state. Then we identify the set $\mathcal{X}_{(1,t)}$ such that if the state lies in this set, then it is beneficial for the jammer to jam the control signal. Then we move on the next step $t+1$ until the entire horizon N is covered. ■

The following proposition can be proved, in complete analogy to Proposition 3.4.

Proposition 3.8 $\lim_{|x|\to\infty} \tau_{(1,t)}(x)$ *exists and is equal to*

$$\sqrt{\frac{\kappa^{1,J}_{(1,t-1)} + \kappa^{2,J}_{(1,t-1)} - \kappa^{2,J}_{(1,t)}}{\kappa^{1,J}_{(1,t)} - \left(1 + A^2\frac{\kappa^{1,J}_{(1,t-1)}}{1+\kappa^{1,J}_{(1,t-1)}}\right)}}\sigma_w.$$

Proof: Using the same technique as in Lemma 3.3, we can prove

$$\left.\frac{d\mathscr{J}^C_{(1,t)}}{du_{(1,t)}}\right|_{u_{(1,t)}=-Ax_{(1,t)}} = 2u_{(1,t)} = -2Ax_{(1,t)} \neq 0, \quad (3.36)$$

which implies $L_{(1,t)}(x_{(1,t)}) \neq 1 \; \forall \; x_{(1,t)} \neq 0$. Therefore, as state $|x_{(1,t)}| \to \infty$, $|Ax_{(1,t)} + \tilde{\gamma}^*(x_{(1,t)}, 1, t)^*| \to \infty$ also holds. Let us see the behavior of $L_{(1,t)}(x_{(1,t)})$ as state $x_{(1,t)}$ becomes large. Taking the limit $|x_{(1,t)}| \to \infty$ in (3.28) and (3.29), we get

$$\lim_{|x_{(1,t)}|\to\infty} P_{(1,t)}(x_{(1,t)}, \tilde{\gamma}^*(x_{(1,t)}, 1, t)) = 1,$$
$$\lim_{|x_{(1,t)}|\to\infty} R_{(1,t)}(x_{(1,t)}, \tilde{\gamma}^*(x_{(1,t)}, 1, t)) = 1.$$

We know from our discussion in the last section, that $\kappa^{1,C}_{(1,t)}$ and $\kappa^{2,C}_{(1,t)}$ are even functions of the state $x_{(1,t)}$. We exploit this symmetry and take the limit in (3.30) and (3.31), the values of $\psi^1_{(1,t)}(x_{(1,t)}, \tilde{\gamma}^*(x_{(1,t)}, 1, t))$ and $\psi^2_{(1,t)}(x_{(1,t)}, \tilde{\gamma}^*(x_{(1,t)}, 1, t))$ are

$$\lim_{|x_{(1,t)}|\to\infty} \psi^1_{(1,t)}(x_{(1,t)}, \tilde{\gamma}^*(x_{(1,t)}, 1, t)) = \kappa^{1,J}_{(1,t-1)},$$
$$\lim_{|x_{(1,t)}|\to\infty} \psi^2_{(1,t)}(x_{(1,t)}, \tilde{\gamma}^*(x_{(1,t)}, 1, t)) = \kappa^{2,J}_{(1,t-1)}.$$

The derivative terms in (3.32) converge to 0 in the limit

$$\lim_{|x_{(1,t)}|\to\infty} \left((Ax_{(1,t)} + u_{(1,t)})^2 + \sigma_w^2\right) \left.\frac{d\psi^1_{(1,t)}}{du_{(1,t)}}\right|_{u_{(1,t)}=\tilde{\gamma}^*(x_{(1,t)},1,t)} = 0,$$
$$\lim_{|x_{(1,t)}|\to\infty} \left.\frac{d\psi^2_{(1,t)}}{du_{(1,t)}}\right|_{u_{(1,t)}=\tilde{\gamma}^*(x_{(1,t)},1,t)} = 0.$$

Using these relations in (3.32) at optimal control $u^*_{(1,t)}$, we get

$$\lim_{|x_{(1,t)}|\to\infty} \frac{1}{Ax_{(1,t)}} \left.\frac{d\mathscr{J}^C_{(1,t)}(x_{(1,t)}, u_{(1,t)})}{du_{(1,t)}}\right|_{u_{(1,t)}=\tilde{\gamma}^*(x_{(1,t)},1,t)} = 0,$$
$$\lim_{|x_{(1,t)}|\to\infty} -2L_{(1,t)}(x_{(1,t)}) + 2(1 - L_{(1,t)}(x_{(1,t)}))\kappa^{1,J}_{(1,t-1)} = 0.$$

This relation yields

$$\lim_{|x_{(1,t)}|\to\infty} L_{(1,t)}(x_{(1,t)}) = \frac{\kappa^{1,J}_{(1,t-1)}}{1 + \kappa^{1,J}_{(1,t-1)}}. \tag{3.37}$$

Putting this limiting value of $L_{(1,t)}$ in (3.33) and (3.34), we get

$$\lim_{|x_{(1,t)}|\to\infty} \kappa^{1,C}_{(1,t)}(x_{(1,t)}) = 1 + A^2 \frac{\kappa^{1,J}_{(1,t-1)}}{1 + \kappa^{1,J}_{(1,t-1)}}, \tag{3.38}$$
$$\lim_{|x_{(1,t)}|\to\infty} \kappa^{2,C}_{(1,t)}(x_{(1,t)}) = \kappa^{1,J}_{(1,t-1)} + \kappa^{2,J}_{(1,t-1)}. \tag{3.39}$$

Taking the limit in (3.35) and substituting (3.38) and (3.39)

$$\lim_{|x_{(1,t)}|\to\infty} \tau_{(1,t)}(x_{(1,t)}) = \sqrt{\frac{\kappa^{1,J}_{(1,t-1)} + \kappa^{2,J}_{(1,t-1)} - \kappa^{2,J}_{(1,t)}}{\kappa^{1,J}_{(1,t)} - \left(1 + A^2 \frac{\kappa^{1,J}_{(1,t-1)}}{1+\kappa^{1,J}_{(1,t-1)}}\right)}}\sigma_w. \tag{3.40}$$

This completes the proof. ∎

3.3 General Case

We now consider the general case, as in Figure 3.2. The current stage is (s,t), which means that there are t time steps to go from now and the jammer can jam s times till the end of the game. If the jammer chooses to jam at stage (s,t), then the next stage is $(s-1,t-1)$. If the jammer chooses not to jam, then the next stage is going to be $(s,t-1)$ (see Figure 3.2). From our previous discussion, we know following facts :

- All κ's are even function of state x for all (s,t)
- As a result, τ's are also even function of state x
- The set $\mathcal{X}_{(s,t)}$ is symmetric with respect to $x=0$ line

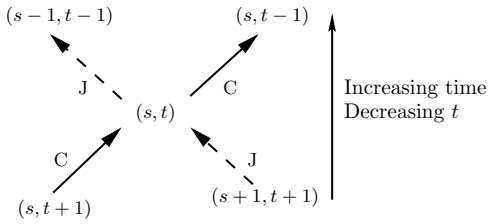


Figure 3.2: Extended state space for a general stage. Here "J" means that the jammer is active at this time instant and "C" means that the controller is active at this time instant.

3.3.1 Cost with Control at stage (s,t)

Let $\mathcal{X}_{(s,t-1)}$ denote the set of all states at stage $(s,t-1)$, in which jamming is a better strategy for the jammer:

$$\mathcal{X}_{(s,t-1)} \quad = \quad \left\{x_{(s,t-1)} \in \mathbb{R} : x^2_{(s,t-1)} - \tau^2_{(s,t-1)}(x_{(s,t-1)}) \geq 0\right\}. \tag{3.41}$$

Let us define $\psi^{1,C}_{(s,t)}(x_{(s,t)},u_{(s,t)})$ and $\psi^{2,C}_{(s,t)}(x_{(s,t)},u_{(s,t)})$ as follows

$$\begin{aligned}
\psi^{1,C}_{(s,t)}(x_{(s,t)},u_{(s,t)}) &= \int_{\mathcal{X}^c_{(s,t-1)}} \frac{\kappa^{1,C}_{(s,t-1)}(x_{(s,t-1)})x^2_{(s,t-1)}}{(Ax_{(s,t)}+u_{(s,t)})^2+\sigma_w^2} \times f(x_{(s,t-1)}|x_{(s,t)},u_{(s,t)})dx_{(s,t-1)} \\
&\quad + \int_{\mathcal{X}_{(s,t-1)}} \frac{\kappa^{1,J}_{(s,t-1)}(x_{(s,t-1)})x^2_{(s,t-1)}}{(Ax_{(s,t)}+u_{(s,t)})^2+\sigma_w^2} f(x_{(s,t-1)}|x_{(s,t)},u_{(s,t)})dx_{(s,t-1)}, \qquad (3.42) \\
\psi^{2,C}_{(s,t)}(x_{(s,t)},u_{(s,t)}) &= \int_{\mathcal{X}^c_{(s,t-1)}} \kappa^{2,C}_{(s,t-1)}(x_{(s,t-1)}) \times f(x_{(s,t-1)}|x_{(s,t)},u_{(s,t)})dx_{(s,t-1)} \\
&\quad + \int_{\mathcal{X}_{(s,t-1)}} \kappa^{2,J}_{(s,t-1)}(x_{(s,t-1)}) \times f(x_{(s,t-1)}|x_{(s,t)},u_{(s,t)})dx_{(s,t-1)}. \qquad (3.43)
\end{aligned}$$

The cost to the controller is given by

$$\begin{aligned}
\mathscr{J}^C_{(s,t)}(x_{(s,t)},u_{(s,t)}) &= x^2_{(s,t)}+u^2_{(s,t)}+\left(Ax_{(s,t)}+u_{(s,t)}\right)^2\psi^{1,C}_{(s,t)}(x_{(s,t)},u_{(s,t)}) \\
&\quad +\sigma_w^2\left(\psi^{1,C}_{(s,t)}(x_{(s,t)},u_{(s,t)})+\psi^{2,C}_{(s,t)}(x_{(s,t)},u_{(s,t)})\right).
\end{aligned}$$

From Lemma 3.6 above, first order necessary condition for optimality is also sufficient. Differentiating it with respect to $u_{(s,t)}$, we get

$$\frac{d\mathscr{J}^C_{(s,t)}}{du_{(s,t)}} = 2u_{(s,t)}+2\left(Ax_{(s,t)}+u_{(s,t)}\right)\psi^{1,C}_{(s,t)}+\left(Ax_{(s,t)}+u_{(s,t)}\right)^2\frac{d\psi^{1,C}_{(s,t)}}{du_{(s,t)}}+\sigma_w^2\left(\frac{d\psi^{1,C}_{(s,t)}}{du_{(s,t)}}+\frac{d\psi^{2,C}_{(s,t)}}{du_{(s,t)}}\right), \quad (3.44)$$

which vanish at the optimal value of control $\tilde{\gamma}^*(x_{(s,t)},s,t)$,

$$\frac{d\mathscr{J}^C_{(s,t)}}{du_{(s,t)}}\left(x_{(s,t)},\tilde{\gamma}^*(x_{(s,t)},s,t)\right) = 0.$$

This way, we get the optimal control as a function of the state at this stage. Again, define $L_{(s,t)}(x_{(s,t)}) = -\tilde{\gamma}^*(x_{(s,t)},s,t)/(Ax_{(s,t)})$. Then the coefficient for the optimal cost at stage (s,t) if the jammer chooses not to jam is given by

$$\begin{aligned}
\kappa^{1,C}_{(s,t)}(x_{(s,t)}) &= 1+A^2\left(L^2_{(s,t)}(x_{(s,t)})+(1-L_{(s,t)}(x_{(s,t)}))^2\psi^{1,C}_{(s,t)}\left(x_{(s,t)},\tilde{\gamma}^*(x_{(s,t)},s,t)\right)\right), \qquad (3.45) \\
\kappa^{2,C}_{(s,t)}(x_{(s,t)}) &= \psi^{1,C}_{(s,t)}\left(x_{(s,t)},\tilde{\gamma}^*(x_{(s,t)},s,t)\right)+\psi^{2,C}_{(s,t)}\left(x_{(s,t)},\tilde{\gamma}^*(x_{(s,t)},s,t)\right). \qquad (3.46)
\end{aligned}$$

3.3.2 Cost with Jamming at stage (s,t)

Let us define $\psi^{1,J}_{(s,t)}(x_{(s,t)})$ and $\psi^{2,J}_{(s,t)}(x_{(s,t)})$ as follows :

$$\begin{aligned}
\psi^{1,J}_{(s,t)}(x_{(s,t)}) &= \int_{\mathcal{X}^c_{(s-1,t-1)}} \frac{\kappa^{1,C}_{(s-1,t-1)}(x_{(s-1,t-1)})x^2_{(s-1,t-1)}}{(Ax_{(s,t)})^2+\sigma_w^2} \times f(x_{(s-1,t-1)}|x_{(s,t)})dx_{(s-1,t-1)} \\
&\quad + \int_{\mathcal{X}_{(s-1,t-1)}} \frac{\kappa^{1,J}_{(s-1,t-1)}(x_{(s-1,t-1)})x^2_{(s-1,t-1)}}{(Ax_{(s,t)})^2+\sigma_w^2} \times f(x_{(s-1,t-1)}|x_{(s,t)})dx_{(s-1,t-1)}, \quad (3.47) \\
\psi^{2,J}_{(s,t)}(x_{(s,t)}) &= \int_{\mathcal{X}^c_{(s-1,t-1)}} \kappa^{2,C}_{(s-1,t-1)}(x_{(s-1,t-1)}) \times f(x_{(s-1,t-1)}|x_{(s,t)})dx_{(s-1,t-1)} \\
&\quad + \int_{\mathcal{X}_{(s-1,t-1)}} \kappa^{2,J}_{(s-1,t-1)}(x_{(s-1,t-1)}) \times f(x_{(s-1,t-1)}|x_{(s,t)})dx_{(s-1,t-1)}. \quad (3.48)
\end{aligned}$$

The cost to the controller is given by

$$J^J_{(s,t)}(x_{(s,t)}) = x^2_{(s,t)} + \left(Ax_{(s,t)}\right)^2 \psi^{1,J}_{(s,t)}(x_{(s,t)}) + \sigma_w^2 \left(\psi^{1,J}_{(s,t)}(x_{(s,t)}) + \psi^{2,J}_{(s,t)}(x_{(s,t)})\right).$$

Then the coefficient for the optimal cost at stage (s,t) if the jammer chooses to jam is given by

$$\begin{aligned}
\kappa^{1,J}_{(s,t)}(x_{(s,t)}) &= 1 + A^2\psi^{1,J}_{(s,t)}(x_{(s,t)}), \quad (3.49) \\
\kappa^{2,J}_{(s,t)}(x_{(s,t)}) &= \psi^{1,J}_{(s,t)}(x_{(s,t)}) + \psi^{2,J}_{(s,t)}(x_{(s,t)}). \quad (3.50)
\end{aligned}$$

3.3.3 Threshold at stage (s,t)

The threshold at this stage is given by

$$\tau_{(s,t)}(x_{(s,t)}) = \sqrt{\frac{\kappa^{2,C}_{(s,t)}(x_{(s,t)}) - \kappa^{2,J}_{(s,t)}(x_{(s,t)})}{\kappa^{1,J}_{(s,t)}(x_{(s,t)}) - \kappa^{1,C}_{(s,t)}(x_{(s,t)})}}\sigma_w. \quad (3.51)$$

Again, we can find the set

$$\mathcal{X}_{(s,t)} = \left\{x_{(s,t)} : x^2_{(s,t)} - \tau^2_{(s,t)}(x_{(s,t)}) \geq 0\right\}.$$

It should be noted that the constraint on the number of actions the jammer can take during the game is upper bounded by M. It is intuitive that it is in the best interest of the jammer to exhaust all his jamming actions by the end of the horizon. By jamming, the jammer increases the state of the system which adds to the cost of the system. We now prove this intuitive result which explains why the jammer exhausts all his jamming actions available to him at the beginning of the game.

Lemma 3.9 *The value functions are increasing functions of t and $0 \leq s \leq t$, i.e.*

$$\begin{aligned}
V_{(s,t)}(x) &< V_{(s+1,t)}(x) \quad \textit{for} \quad 0 \leq s \leq t-1, \\
V_{(s,t)}(x) &< V_{(s,t+1)}(x) \quad \textit{for} \quad t \geq s
\end{aligned}$$

for all values of $x \in \mathbb{R}$.

Proof: We again employ the principle of induction to prove this lemma. The base case is that of $(0,1)$ and $(1,1)$. We showed in the Section 3.1, $V_{(0,1)}(x) < V_{(1,1)}(x)$ for all values of $x \in \mathbb{R}$. Also note that the value function is increasing as t increases for stages $(0,t)$ and (t,t) as shown below

$$\begin{aligned}
V_{(0,t+1)}(x) &= \inf_u x^2 + u^2 + E\left\{V_{(0,t)}(Ax+u+w)\right\} = \left(1 + A^2 \frac{\kappa^{1,C}_{(0,t)}}{1+\kappa^{1,C}_{(0,t)}}\right) x^2 + \left(\kappa^{1,C}_{(0,t)} + \kappa^{2,C}_{(0,t)}\right)\sigma_w^2 \\
&> \kappa^{1,C}_{(0,t)} x^2 + \kappa^{2,C}_{(0,t)}\sigma_w^2 = V_{(0,t)}(x), \\
V_{(t+1,t+1)}(x) &= x^2 + E\left\{V_{(t,t)}(Ax+w)\right\} = \left(1 + A^2\kappa^{1,J}_{(t,t)}\right) x^2 + \left(\kappa^{1,J}_{(t,t)} + \kappa^{2,J}_{(t,t)}\right)\sigma_w^2 \\
&> \kappa^{1,J}_{(t,t)} x^2 + \kappa^{2,J}_{(t,t)}\sigma_w^2 = V_{(t,t)}(x).
\end{aligned}$$

Next, we prove that $V_{(0,t)}(x) < V_{(1,t)}(x)$ for $t \geq 2$.

$$\begin{aligned}
V_{(1,t)}(x) &= \max\{x^2 + E\{V_{(0,t-1)}(Ax+w)\}, \inf_u x^2 + u^2 + E\{V_{(1,t-1)}(Ax+u+w)\}\}, \\
&> \inf_u x^2 + u^2 + E\{V_{(0,t-1)}(Ax+u+w)\} = V_{(0,t)}(x).
\end{aligned}$$

This holds from the property of maximum and the fact that the cost with control is always better than the cost without control. Now let us assume that $V_{(s-1,t-1)}(x) < V_{(s,t-1)}(x) < V_{(s+1,t-1)}(x)$ for all $x \in \mathbb{R}$ and for $s \geq 1$. Then, from the positivity of probability distribution, we get

$$\begin{aligned}
V_{(s+1,t)}(x) &= \max\{J^J_{(s+1,t)}(x), J^C_{(s+1,t)}(x)\}, \\
&= \max\{x^2 + E\{V_{(s,t-1)}(Ax+w)\}, \inf_u x^2 + u^2 + E\{V_{(s+1,t-1)}(Ax+u+w)\}\}, \\
&> \max\{x^2 + E\{V_{(s-1,t-1)}(Ax+w)\}, \inf_u x^2 + u^2 + E\{V_{(s,t-1)}(Ax+u+w)\}\}, \\
&= V_{(s,t)}(x).
\end{aligned}$$

Using similar argument, we can prove that $V_{(s,t)}(x) < V_{(s,t+1)}(x)$ for all $x \in \mathbb{R}$ and $2 \leq s \leq t$. This completes the induction step and we prove the lemma. ∎

3.4 Multidimensional State Space

Let us consider the case when the state and control actions of the plant are multi-dimensional. The state equation under adversarial jamming evolves as

$$x_{k+1} = Ax_k + \alpha_k B u_k + w_k\,, \qquad k = 0, 1, ..., N-1\,, \tag{3.52}$$

where $x_k \in \mathbb{R}^n$ is the state of the plant, $u_k \in \mathbb{R}^m$ is the control signal, $\{w_k\}$ is an n-dimensional discrete-time zero mean Gaussian random vector with variance Σ_w (i.e. $w_k \sim \mathcal{N}(0, \Sigma_w)$). The initial state x_0 is also an n-dimensional zero mean Gaussian random vector with variance Σ_0, and is assumed to be independent of the noise process $\{w_k\}$. Here, $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$ are matrices with real entries.

Similar to the formulation in Chapter 2, the sequence $\{\alpha_k \in \{0,1\}\}$ is the control of the jammer, where $\alpha_k = 0$ means that the jammer is active at time k and no control action is applied to the plant, whereas $\alpha_k = 1$ means that the jammer is inactive and the control action is applied to the plant. The assumption that the jammer is allowed to intercept at most M times (in a horizon of N), is captured by the jammer constraint $\sum_{k=0}^{N-1}(1-\alpha_k) = M$.

Again, we consider a quadratic cost function for the plant, which is given by

$$J = \sum_{k=1}^{N-1} \left(x_k^T Q x_k + \alpha_k u_k^T R u_k\right) + x_N^T Q x_N,$$

where $Q \geq 0$ and $R > 0$ are matrices of appropriate dimensions.

In this section, we derive the underlying equations for the case when $M = 1$ and $N = 2$. At stage $(0,0)$, the cost is

$$J_{(0,0)}(x_2) = x_2^T Q x_2.$$

At stage $(0,1)$, the jammer has no chance to jam and the controller's signal is applied to the system. The expected cost is

$$J_{(0,1)}(x_1) = x_1^T \left(A^T Q A + Q - A^T Q B (R + B^T Q B)^{-1} B^T Q A\right) x_1 + \operatorname{tr}\left(Q \Sigma_w\right).$$

The control signal at this stage is

$$\tilde{\gamma}^*(x,0,1) = -\left((R + B^T Q B)^{-1} B^T Q A\right) x.$$

Let us denote

$$\kappa_{(0,1)}^{1,C} = \left(A^T Q A + Q - A^T Q B (R + B^T Q B)^{-1} B^T Q A\right), \qquad \kappa_{(0,1)}^{2,C} = Q,$$

such that the cost at this stage becomes

$$J_{(0,1)}(x_1) = x_1^T \kappa_{(0,1)}^{1,C} x_1 + \operatorname{tr}\left(\kappa_{(0,1)}^{2,C} \Sigma_w\right).$$

At stage $(1,1)$, the expected cost is

$$J_{(1,1)}(x_1) = x_1^T \left(A^T Q A + Q\right) x_1 + \operatorname{tr}\left(Q \Sigma_w\right).$$

Similarly, define

$$\kappa_{(1,1)}^{1,J} = \left(A^T Q A + Q\right), \qquad \kappa_{(1,1)}^{2,J} = Q,$$

and the cost is

$$J_{(1,1)}(x_1) = x_1^T \kappa_{(1,1)}^{1,J} x_1 + \operatorname{tr}\left(\kappa_{(1,1)}^{2,J} \Sigma_w\right).$$

Consider stage $(1,2)$. We will have two cases. The cost with jamming at stage $(1,2)$ is

$$J^J_{(1,2)}(x_0) = x_0^T \mathcal{R}^J \left(\kappa^{1,C}_{(0,1)}\right) x_0 + \operatorname{tr}\left(\left(\kappa^{1,C}_{(0,1)} + \kappa^{2,C}_{(0,1)}\right)\Sigma_w\right),$$

and without jamming is

$$J^C_{(1,2)}(x_0) = x_0^T \mathcal{R}^C \left(\kappa^{1,J}_{(1,1)}\right) x_0 + \operatorname{tr}\left(\left(\kappa^{1,J}_{(1,1)} + \kappa^{2,J}_{(1,1)}\right)\Sigma_w\right).$$

The optimal control at this stage is given by

$$\tilde{\gamma}^*(x,1,2) = -\left((R + B^T\kappa^{1,J}_{(1,1)}B)^{-1}B^T\kappa^{1,J}_{(1,1)}A\right)x.$$

The difference in the cost gives us the threshold hyper-surface for each stage which is the set of all $x_0 \in \mathbb{R}^n$ such that

$$x_0^T\left(\mathcal{R}^J\left(\kappa^{1,C}_{(0,1)}\right) - \mathcal{R}^C\left(\kappa^{1,J}_{(1,1)}\right)\right)x_0 + \operatorname{tr}\left(\left(\kappa^{1,C}_{(0,1)} - \kappa^{1,J}_{(1,1)}\right)\Sigma_w\right) = 0. \tag{3.53}$$

This surface denotes an ellipsoid in the n-dimensional state space with the center at origin. In the interior of the ellipsoid (which contains the origin), the expected cost with control is greater than the expected cost with jamming. Hence, the jammer chooses to remain inactive and the controller controls the plant. Outside the region which extends to infinity, the optimal expected cost with jamming is greater than the expected cost with control. Therefore, the jammer chooses to jam if the state lies outside the ellipsoid.

We considered the case $M = 1$ and $N = 2$ in this section. For a general (M, N), we can proceed in a similar way to calculate the region of jamming and not jamming at all stages. However, it is not hard to see that after stage $(1,2)$, the computation of optimal expected cost and optimal control strategies requires integration over n-dimensional space, which is computationally intensive.

3.5 Numerical Simulations

As a result of using dynamic programming for this problem, we get a strongly time consistent strategy for both the players. By strong time consistency, we mean that the solution of the problem remains unchanged from any stage (s,t) till the stage $(0,0)$, and the strategy does not depend on the history of jamming and control actions until the stage (s,t).

In this section, we discuss some simulation results which we obtained for various values of parameters A and σ_w for the scalar case as studied in Section 3.2. All simulations were performed in MATLAB. Integration of value functions were performed using the standard `ode45` function of MATLAB. Since the integration can not be performed till ∞, the upper limit of integration was taken to be $|Ax + u| + 10\sigma_w$ (and lower limit was $-(|Ax + u| + 10\sigma_w)$). The maximum step size for integration was limited to $5\sigma_w$ to achieve desired accuracy. For calculating the infimum of the cost function, differentiation was performed numerically and `fzero` function was invoked to find the control value at infimum. Then the threshold was calculated using the algorithm described in this chapter.

Figure 3.3 shows the set $\mathcal{X}_{(1,t)}$ for t ranging from 2 to 12 for an unstable system with $A = 2.5$ and $\sigma_w = 1$.

In Figure 3.3, at a fixed integer N, the darker region indicates the set $\mathcal{X}_{(1,N)}$ and lighter region indicates the set $\mathcal{X}^c_{(1,N)}$. The bold line in the graph is the boundary of the set $\mathcal{X}_{(1,N)}$. The vertical line extends to ∞ above and $-\infty$ below. This set can be computed off line and stored with the jammer.

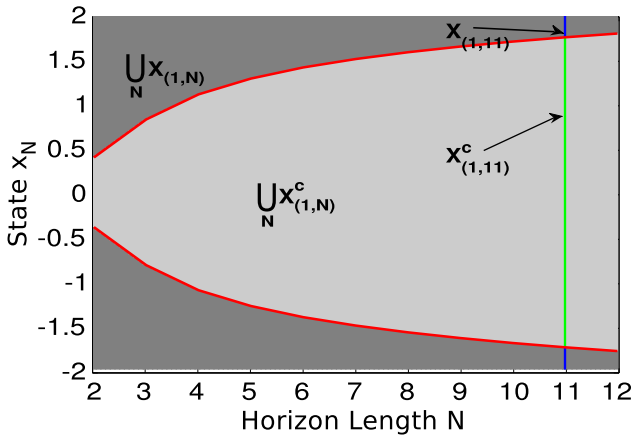


Figure 3.3: Region showing the union of the sets in which the jammer jams and does not jam as a function of horizon length N.

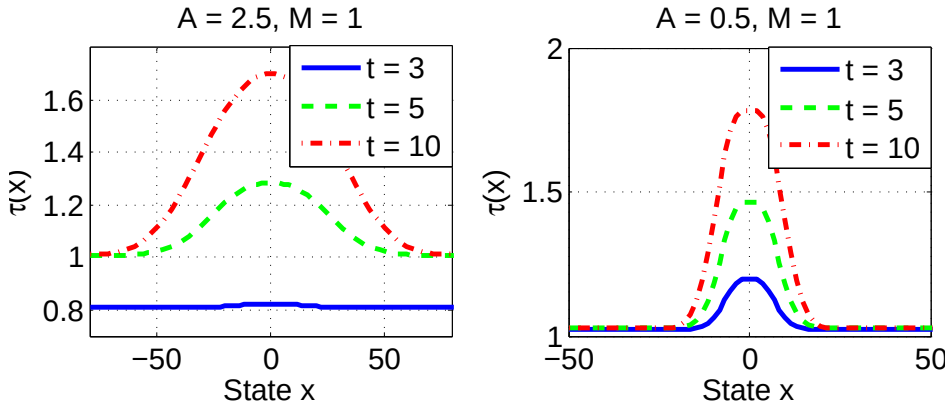


Figure 3.4: Variations in $\tau_{(1,t)}(x_{(1,t)})$ as a function of state $x_{(1,t)}$ for an unstable system with $A = 2.5$, $\sigma_w = 1$ and for a stable system with $A = 0.5$, $\sigma_w = 1$ for $t = 3, 5, 10$.

The two sets of graphs of Figure 3.4 show the values of $\tau_{(1,t)}(x)$ for various values of t and x. It should be noted that for an N-stage problem, the threshold function $\tau_{(1,t)}(x)$, $t < N$, is the same as $\tau_{(1,t)}(x)$ for a t-stage problem. As can be observed from these curves, and similarly to the $M = 1, N = 3$ case, these threshold functions have a limit as the state goes to infinity.

Expanding the present analysis to $M \geq 2$ seems to be quite challenging numerically. As derived in this chapter, $\kappa^{1,J}_{(s,t)}$ and $\kappa^{2,J}_{(s,t)}$ are functions of state $x_{(s,t)}$ for this case. The values of $\psi^1_{(s,t)}$ and $\psi^1_{(s,t)}$ involve multiple integrals over the set $\mathcal{X}_{(s,t)}$ and $\mathcal{X}^c_{(s,t)}$ (see (3.42), (3.43), (3.47) and (3.48)). Due to the nonlinear nature of the integrals and differentiation, closed-form solution for the threshold is not possible even for the simple case of $M = 1$ and $N = 3$. One has to switch to computational methods to compute the set $\mathcal{X}_{(s,t)}$, in which the jammer must jam in order to increase the cost. It is seen that the jammer's policy is not to jam

when the state is "small", and to jam when the state is "large". This result holds true for $M \geq 2$ case too. For intermediate values of state, the accurate value of the threshold is needed.

In multi-dimensional state space, the regions of jamming and not jamming are separated by a hyper-surface, and their analysis involves integrating the Gaussian distribution in a multi-dimensional space over the regions within the hyper-surface and outside the hyper-surface. This makes the computation and analysis of jammer's policy even more difficult than in the scalar case. Extending the result from single dimension to the multi-dimensional state space, the jammer must jam if the state is "large", and not jam if the state is sufficiently "small".

In this chapter, we studied the jamming problem for the case when there was no constraint on the state of the system. In the next chapter, we will consider the jamming problem with a state constraint on the system at each time step.

CHAPTER 4

OPTIMAL CONTROL WITH STATE CONSTRAINTS

This chapter is an extension of the previous chapter. Our formulation, detailed in Chapter 2, considers a dynamic zero-sum game between the jammer and the controller with a constraint on the state. We show that saddle-point equilibrium strategies exist and use dynamic programming to compute them. In particular, we show that the jammer saddle-point equilibrium strategy is threshold-based, which means that at every time step, the jammer jams if and only if the plant's state is larger than an off-line computable and time-varying threshold. Our main result is given in Section 4.1. We calculate the value functions and the optimal strategy for a simple situation in Section 4.2, in which the jammer can only act once over a 2-steps horizon. In Section 4.3, we discuss the relationship with the results of Chapter 3. In Section 4.4, we compute the threshold values numerically for various cases.

4.1 Main Result

In this section, we start with calculating the expected cost and optimal strategy for each of the players for the game formulated in Chapter 2. Let us assume that the game is currently at stage (s,t), where $0 < s < t$. Then the next stage of the game could be $(s-1, t-1)$ or $(s, t-1)$ depending upon whether the jammer was active or not.

Let us consider the case that the jammer is inactive. Denote the current state as x and the control variable as u. The expected cost of the game given the information I_{N-t} is

$$J_{(s,t,\varrho)}(x,u,1) = E\{x^2 + u^2 + V_{(s,t-1,\varrho)}(Ax+u+w)|I_{N-t}\}$$

We wish to minimize the cost using some control action u subjected to the constraint

$$|E\{x_{(s,t-1)}|I_{N-t}\}| = |Ax+u| \leq \varrho.$$

The Lagrangian of the underlying optimization problem is given by

$$L(x,u,\lambda_1,\lambda_2) \quad = \quad J_{(s,t,\varrho)}(x,u,1) + \lambda_1(Ax+u-\varrho) - \lambda_2(Ax+u+\varrho).$$

The Karush-Kuhn-Tucker conditions for this optimization problem is

$$\begin{aligned}
\frac{\partial L}{\partial u}(x, u^*, \lambda_1, \lambda_2) &= 0, \\
\lambda_i &\geq 0 \quad \text{for } i = 1, 2, \\
\lambda_1(Ax + u^* - \varrho) &= 0, \\
\lambda_2(Ax + u^* + \varrho) &= 0.
\end{aligned}$$

When the constraint is not active, the optimal control is

$$u^*(x) = u^*_{(s,t)}(x) = \arg\min_u J_{(s,t,\varrho)}(x, u, 1)$$

and $\lambda_1 = \lambda_2 = 0$. When the constraint is active, then

$$u^*(x) = \begin{cases} \varrho - Ax & \text{if } Ax + u^*_{(s,t)}(x) > \varrho, \\ -\varrho - Ax & \text{if } Ax + u^*_{(s,t)}(x) < -\varrho. \end{cases}$$

Therefore, the controller's optimal strategy is

$$\tilde{\gamma}^*(x, \varrho, s, t) = \begin{cases} u^*_{(s,t)}(x) & \text{if } |Ax + u^*_{(s,t)}(x)| \leq \varrho \\ \varrho - Ax & \text{if } Ax + u^*_{(s,t)}(x) > \varrho \\ -\varrho - Ax & \text{if } Ax + u^*_{(s,t)}(x) < -\varrho \end{cases}. \tag{4.1}$$

As introduced in the Section 2.3 in Chapter 2, the expected cost with optimal control $u^*_{(s,t)}(x)$ is denoted by $J^C_{(s,t,\varrho)}(x)$. Now, let us consider that the jammer is active. The expected cost of the game is

$$J^J_{(s,t,\varrho)}(x) = x^2 + E\{V_{(s-1,t-1),\varrho)}(Ax + w)\}.$$

Additionally, the state constraint restricts the jammer to be active only when

$$|E\{x_{(s-1,t-1)}|I_{N-t}\}| = |Ax| \leq \varrho.$$

Therefore, the jammer's optimal strategy is given by

$$\tilde{\mu}^*(x, \varrho, s, t) = \begin{cases} 0 & \text{if } J^J_{(s,t,\varrho)}(x) \geq J^C_{(s,t,\varrho)}(x) \text{ and } |Ax| \leq \varrho \\ 1 & \text{if } J^J_{(s,t,\varrho)}(x) < J^C_{(s,t,\varrho)}(x) \text{ or } |Ax| > \varrho \end{cases}.$$

The jammer chooses to jam when the cost with jamming $J^J_{(s,t,\varrho)}(x)$ is greater than the cost with control $J^C_{(s,t,\varrho)}(x)$ and also when he satisfies the state constraint. Notice that the set of values of state x where the jammer jams is a subset of the set of values of x where the controller applies optimal control without active constraint. This is because $u^*_{(s,t)}(x)$ is minimizing a quadratic cost and driving the state of the system to zero resulting in $|Ax + u^*_{(s,t)}(x)| < |Ax|$. The value function of the game is calculated to be

$$V_{(s,t,\varrho)}(x) = \begin{cases} J^J_{(s,t,\varrho)}(x) & \text{if } |Ax| \leq \varrho \text{ and} J^J_{(s,t,\varrho)}(x) \geq J^C_{(s,t,\varrho)}(x) \\ J_{(s,t,\varrho)}(x, u^*(x), 1) & \text{otherwise} \end{cases},$$

where $u^*(x) = \tilde{\gamma}^*(x, \varrho, s, t)$. Now let us consider the case when the jammer has no chance left to jam and $s = 0$. The optimal control in this case remains the same as calculated earlier in (4.1) with s replaced by 0. The jammer remains inactive and the value function is given by

$$V_{(0,t,\varrho)}(x) = J_{(0,t,\varrho)}(x, \tilde{\gamma}^*(x, \varrho, 0, t), 1).$$

When the jammer has $s = t$ jamming instances left, then he can jam the system till the end of the horizon. However, he must also satisfy the state constraint. On instances when the jammer could not exercise his jamming action due to active constraint, the next stage considered is $(t-1, t-1)$ (instead of $(t, t-1)$, since the jammer can jan $t-1$ times only). The optimal strategy for the jammer is

$$\tilde{\mu}^*(x, \varrho, t, t) = \begin{cases} 0 & \text{if } |Ax| \leq \varrho \\ 1 & \text{if } |Ax| > \varrho \end{cases}.$$

Again, the controller's strategy can be calculated in a similar manner as above and remains the same as given in (4.1) with the value of s replaced by the value of t. The value of the game is given by

$$V_{(t,t,\varrho)}(x) = \begin{cases} J^J_{(t,t,\varrho)}(x) & \text{if } |Ax| \leq \varrho \\ J_{(s,t,\varrho)}(x, u^*, 1) & \text{otherwise} \end{cases},$$

where $u^* = \tilde{\gamma}^*(x, \varrho, t, t)$. Starting from $V_{(0,0,\varrho)}(x) = x^2$, one can recursively compute the value functons and the strategies of the players in this game. This completes the derivation of saddle-point equilibrium strategy for the jammer and the controller playing the zero-sum game formulated in Chapter 2 with state constraint. In the next section, we will derive the cost and value functions explicitly for the case when the jammer has one chance to jam and the horizon is of length two, i.e. $M = 1$ and $N = 2$.

4.2 The M=1, N=2 case

In this section, we start by computing feedback saddle-point equilibrium strategies $(\tilde{\gamma}^*, \tilde{\mu}^*)$ for the extended game in the simple case where $N = 2$ and $M = 1$ (i.e., the jammer can only jam once in two time steps). For simplicity sake, we assume that $A > 0$. Let us start with the stage $(0, 0)$, which is the end of the horizon. At this stage, by definition, the value function is

$$V_{(0,0,\varrho)}(x) = x^2.$$

At stage $(0, 1)$, the jammer has no chance left to jam. The controller has to choose the optimal control such that it satisfies the state constraint at the next time step. The unconstrained optimal control for the stage is

$$u^*_{(0,1)}(x) = -\frac{A}{2}x.$$

However, with this control, the expected state at the next stage is

$$\hat{y}_{(0,0)}(x) = E\{Ax + u^*_{(0,1)}(x) + w\} = \frac{A}{2}x.$$

If the expected state is above the threshold ϱ, then the controller applies a control so as to satisfy the constraint. Therefore, the saddle-point strategy for the controller in this game at stage $(0,1)$ is

$$\tilde{\gamma}^*(x,\varrho,0,1) = \begin{cases} -\frac{A}{2}x & \text{if } -\frac{2\varrho}{A} \leq x \leq \frac{2\varrho}{A} \\ \varrho - Ax & \text{if } x > \frac{2\varrho}{A} \\ -\varrho - Ax & \text{if } x < -\frac{2\varrho}{A} \end{cases},$$

and the saddle-point value function is given by

$$V_{(0,1,\varrho)}(x) = \begin{cases} V^1_{(0,1,\varrho)}(x) & \text{if } \frac{-2\varrho}{A} \leq x \leq \frac{2\varrho}{A} \\ V^2_{(0,1,\varrho)}(x) & \text{otherwise} \end{cases},$$

where,

$$\begin{aligned} V^1_{(0,1,\varrho)}(x) &= \left(1 + \frac{A^2}{2}\right)x^2 + \sigma_w^2 \\ V^2_{(0,1,\varrho)}(x) &= (1+A^2)x^2 - 2\varrho A|x| + 2\varrho^2 + \sigma_w^2 \end{aligned}$$

Since the jammer has no chance left to jam, the strategy of the jammer is trivially given by

$$\tilde{\mu}^*(x,\varrho,0,1) = 0. \tag{4.2}$$

Next, we consider the stage $(1,1)$. At stage $(1,1)$, the jammer choses to jam if it does not violate the state constraint. Therefore, with an active jammer, the value function is

$$V_{(1,1,\varrho)}(x) = x^2 + E\{(Ax+w)^2|I_1\} = (1+A^2)x^2 + \sigma_w^2,$$

where we used the zero mean property and independence of the noise variable w. However, the jammer can only jam if $Ax \leq \varrho$. Therefore, the value function is

$$V_{(1,1,\varrho)}(x) = \begin{cases} V^1_{(1,1,\varrho)}(x) & \text{if } \frac{-\varrho}{A} \leq x \leq \frac{\varrho}{A} \\ V^1_{(0,1,\varrho)}(x) & \text{if } \frac{\varrho}{A} < |x| \leq \frac{2\varrho}{A} \\ V^2_{(0,1,\varrho)}(x) & \text{otherwise} \end{cases},$$

where

$$V^1_{(1,1,\varrho)}(x) = (1+A^2)x^2 + \sigma_w^2.$$

The optimal strategy for the controller remains the same as in $(0,1)$ case, i.e.,

$$\tilde{\gamma}^*(x,\varrho,1,1) = \begin{cases} -\frac{A}{2}x & \text{if } -\frac{2\varrho}{A} \leq x \leq \frac{2\varrho}{A} \\ \varrho - Ax & \text{if } x > \frac{2\varrho}{A} \\ -\varrho - Ax & \text{if } x < -\frac{2\varrho}{A} \end{cases},$$

while the jammer's strategy is

$$\tilde{\mu}^*(x,\varrho,1,1) = \begin{cases} 0 & \text{if } x \leq \frac{\varrho}{A} \\ 1 & \text{otherwise} \end{cases}.$$

Next, we consider the stage $(1,2)$, which is the initial step of the game. The jammer can either choose to jam now, or jam later in the next step. It must be noted that if the jammer decides to jam now, then he must also satisfy the state constraint. The expected cost at this stage is

$$J^J_{(1,2,\varrho)}(x) = x^2 + E\{V_{(0,1,\varrho)}(Ax+w)|I_0\}. \tag{4.3}$$

The expectation value of the cost at next stage is calculated by following integration

$$\begin{aligned} E\{V_{(0,1,\varrho)}(Ax+w)|I_0\} &= \int_{-2\varrho/A}^{2\varrho/A} V^1_{(0,1,\varrho)}(\tilde{x}) f(\tilde{x}|x) d\tilde{x} + \int_{-\infty}^{-2\varrho/A} V^2_{(0,1,\varrho)}(\tilde{x}) f(\tilde{x}|x) d\tilde{x} \\ &\quad + \int_{2\varrho/A}^{\infty} V^2_{(0,1,\varrho)}(\tilde{x}) f(\tilde{x}|x) d\tilde{x}, \end{aligned}$$

where $f(\tilde{x}|x) = \mathscr{N}(Ax, \sigma_w^2)$ as defined in the earlier section.

Now, let us consider the case when the controller applies the control at the stage $(1,2)$. In this case, the next stage is $(1,1)$, i.e. the jammer has a chance to jam in the future. Therefore, the expected cost for this stage with active controller and inactive jammer is

$$J^C_{(1,2,\varrho)}(x) = \inf_u x^2 + u^2 + E\{V_{(1,1,\varrho)}(Ax+u+w)\}. \tag{4.4}$$

Using the first order necessary condition for optimality, the infimum is calculated by taking the first derivative of the cost function and equating it to zero :

$$\left.\frac{\partial J_{(1,2,\varrho)}(x,u,\alpha=1)}{\partial u}\right|_{u^*_{(1,2)}(x)} = 0.$$

Since the cost function is convex in u from Proposition 3.1, this is also a sufficient condition to obtain the optimal control. This results in the optimal controller's strategy as

$$\tilde{\gamma}^*(x,\varrho,1,2) = \begin{cases} u^*_{(1,2)}(x) & \text{if } |Ax + u^*_{(1,2)}(x)| \leq \varrho, \\ \varrho - Ax & \text{if } Ax + u^*_{(1,2)}(x) > \varrho \\ -\varrho - Ax & \text{if } Ax + u^*_{(1,2)}(x) < -\varrho \end{cases},$$

and the jammer's strategy as

$$\tilde{\mu}^*(x,\varrho,1,2) = \begin{cases} 0 & \text{if } J^J_{(1,2,\varrho)}(x) \geq J^C_{(1,2,\varrho)}(x) \text{ and } |Ax| \leq \varrho \\ 1 & \text{if } J^J_{(1,2,\varrho)}(x) < J^C_{(1,2,\varrho)}(x) \text{ or } |Ax| > \varrho \end{cases} \tag{4.5}$$

Let us define threshold function for the jammer as

$$\tau^c_{(1,2),l} := \{x \in \mathbb{R} : J^J_{(1,2,\varrho)}(x) = J^C_{(1,2,\varrho)}(x)\}, \tag{4.6}$$

$$\tau^c_{(1,2),u} := \frac{\varrho}{A}. \tag{4.7}$$

Here, $\tau^c_{(1,2),l}$ denotes the lower threshold and $\tau^c_{(1,2),u}$ denotes the upper threshold for the jammer for the constrained game. The jammer's strategy is then to jam if the state falls in between these two thresholds.

Now, let us consider the case when the jammer has no choice of jamming and there are two time steps left for the game to end. This corresponds to the stage $(0,2)$. At this stage, the controller controls in order to minimize the expected cost without the jammer's action, but still maintaining the state constraint. The expected cost is

$$J^C_{(0,2,\varrho)}(x) = \inf_u x^2 + u^2 + E\{V_{(0,1,\varrho)}(Ax + u + w)|I_0\}, \tag{4.8}$$

subject to state constraint. Let $u^*_{(0,2)}(x)$ denote the optimal control as a function of the state x in (4.8). Similar to the derivation for optimal control at stage $(1,2)$, the first-order necessary condition for optimality requires that the derivative of $J_{(0,2,\varrho)}(x,u,\alpha=1)$ with respect to u vanish at optimal control $u^*_{(0,2)}(x)$, i.e.

$$\frac{\partial J_{(0,2,\varrho)}(x,u,\alpha=1)}{\partial u}\bigg|_{u^*_{(0,2)}(x)} = 0.$$

The optimal control is then given by

$$\tilde{\gamma}^*(x,\varrho,0,2) = \begin{cases} u^*_{(0,2)}(x) & \text{if } |Ax + u^*_{(0,2)}(x)| \leq \varrho, \\ \varrho - Ax & \text{if } Ax + u^*_{(0,2)}(x) > \varrho, \\ -\varrho - Ax & \text{if } Ax + u^*_{(0,2)}(x) < -\varrho. \end{cases}$$

Having derived the saddle point equilibrium solutions for the controller and the jammer with a constraint on the state, we next discuss the similarity and differences in the solution obtained above and the one obtained in Chapter 3, for the unconstrained state case.

4.3 Discussion on Earlier Results

4.3.1 Characterization of Threshold

The lower threshold as given by (4.6) can only be computed numerically. However, in this sub-section, we compare the lower threshold $\tau^c_{(1,2),l}$ with the unconstrained threshold $\tau_{(1,2)}$ while varying the state constraint and noise variance. At first, we recover the unconstrained threshold as a special case of constrained game

by taking the limit $\varrho \to \infty$. This follows from the three propositions proved below.

Proposition 4.1 *Let $\mathcal{I}_X := [-X, X]$ and $\mathcal{I}_U := [-U, U]$ be two bounded subsets of $\mathbb{R}$. Define*

$$\begin{aligned} J_{(1,2,\infty)}(x,u,1) &:= x^2 + u^2 + \int_{-\infty}^{\infty} V^1_{(1,1,\varrho)}(\tilde{x}) f(\tilde{x}|x,u) d\tilde{x}, \\ J_{(1,2,\infty)}(x,u,0) &:= x^2 + \int_{-\infty}^{\infty} V^1_{(0,1,\varrho)}(\tilde{x}) f(\tilde{x}|x,u) d\tilde{x}. \end{aligned}$$

Then for every $\epsilon > 0$, there exists $\overline{\varrho}_1, \overline{\varrho}_2 \in \mathbb{R}$, such that the cost function with control and without control for the constrained case satisfies

$$\begin{aligned} |J_{(1,2,\infty)}(x,u,1) - J_{(1,2,\varrho)}(x,u,1)| < \epsilon \quad \forall \varrho > \overline{\varrho}_1 \\ |J_{(1,2,\infty)}(x,u,0) - J_{(1,2,\varrho)}(x,u,0)| < \epsilon \quad \forall \varrho > \overline{\varrho}_2 \end{aligned}$$

for all $x \in \mathcal{I}_X$ and $u \in \mathcal{I}_U$.

Proof: Consider $\epsilon > 0$, $x \in \mathcal{I}_X$ and $u \in \mathcal{I}_U$. The cost function at stage $(1,2)$ with control is

$$J_{(1,2,\varrho)}(x,u,1) = x^2 + u^2 + E\{V_{(1,1,\varrho)}(Ax + u + w)|I_0\}.$$

Let us consider the difference between the two cost functions $|J_{(1,2,\infty)}(x,u,1) - J_{(1,2,\varrho)}(x,u,1)|$. After cancellations and using traingle inequality, the difference is

$$\begin{aligned} |J_{(1,2,\infty)}(x,u,1) - J_{(1,2,\varrho)}(x,u,1)| \leq & \int_{-2\varrho/A}^{-\varrho/A} \frac{A^2\tilde{x}^2}{2} f(\tilde{x}|x,u) d\tilde{x} + \int_{\varrho/A}^{2\varrho/A} \frac{A^2\tilde{x}^2}{2} f(\tilde{x}|x,u) d\tilde{x} \\ & + \int_{-\infty}^{-2\varrho/A} |(2\varrho A|\tilde{x}| - 2\varrho^2)| f(\tilde{x}|x,u) d\tilde{x} \\ & + \int_{2\varrho/A}^{\infty} |(2\varrho A|\tilde{x}| - 2\varrho^2)| f(\tilde{x}|x,u) d\tilde{x}. \end{aligned}$$

The first term in the integration is bounded above by

$$\begin{aligned} \int_{-2\varrho/A}^{-\varrho/A} \frac{A^2\tilde{x}^2}{2} f(\tilde{x}|x,u) d\tilde{x} &\leq \frac{2\varrho^2}{\sqrt{2\pi}\sigma_w} e^{\left(-\frac{(\varrho/A - |AX+U|)^2}{2\sigma_w^2}\right)} \\ &< \epsilon/4 \quad \forall \varrho > \varrho_1 \in \mathbb{R}, \end{aligned}$$

for $x \in \mathcal{I}_X$ and $u \in \mathcal{I}_U$. This holds because the upper bound converges to zero as $\varrho \to \infty$. Similarly, the second term is bounded by

$$\int_{\varrho/A}^{2\varrho/A} \frac{A^2\tilde{x}^2}{2} f(\tilde{x}|x,u) d\tilde{x} < \epsilon/4 \quad \forall \varrho > \varrho_2 \in \mathbb{R}.$$

The last two integrals are converging integrals, since each is an integration of product of a polynomial function with an exponentially decaying function. Hence, the values must get arbitrarily small as the interval of the

integration is increased from $2\varrho/A$:

$$\int_{-\infty}^{-2\varrho/A} |(2\varrho A|\tilde{x}| - 2\varrho^2)|f(\tilde{x}|x,u)d\tilde{x} < \epsilon/4, \quad \forall \varrho > \varrho_3 \in \mathbb{R},$$
$$\int_{2\varrho/A}^{\infty} |(2\varrho A|\tilde{x}| - 2\varrho^2)|f(\tilde{x}|x,u)d\tilde{x} < \epsilon/4, \quad \forall \varrho > \varrho_4 \in \mathbb{R}.$$

Now, consider $\overline{\varrho}_1 = \max\{\varrho_1, \varrho_2, \varrho_3, \varrho_4\}$, $x \in \mathcal{I}_X$ and $u \in \mathcal{I}_U$. Then, the difference in the cost is

$$|J_{(1,2,\infty)}(x,u,1) - J_{(1,2,\varrho)}(x,u,1)| < \epsilon \quad \forall \varrho > \overline{\varrho}_1.$$

Using similar techniques as employed above, we can prove the following result for the cost without control

$$|J_{(1,2,\infty)}(x,u,0) - J_{(1,2,\varrho)}(x,u,0)| < \epsilon \quad \forall \varrho > \overline{\varrho}_2.$$

Hence, the cost function for the constrained game converges to the cost function for unconstrained game as $\varrho \to \infty$ when x and u belongs to a compact subset of real line. ∎

Proposition 4.2 *Let $h : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ and $H : \mathbb{R} \to \mathbb{R}$ be continuous functions and $\mathcal{I} \subset \mathbb{R}$ be a closed and bounded set. Assume that for every $\epsilon > 0$, there exists $\varrho_\epsilon \in \mathbb{R}$ such that*

$$|h(u,\varrho) - H(u)| < \epsilon \quad \forall \varrho > \varrho_\epsilon$$

holds for all $u \in \mathcal{I}$. Then,

$$\lim_{\varrho \to \infty} \inf_u h(u,\varrho) = \inf_u H(u), \tag{4.9}$$

i.e., the order of limit and infimum can be interchanged.

Proof: From the statement above, for $\epsilon > 0$, there exists $\varrho_\epsilon \in \mathbb{R}$ such that

$$H(u) - \epsilon < h(u,\varrho) < H(u) + \epsilon \tag{4.10}$$

holds for all $\varrho > \varrho_\epsilon$ and for all $u \in \mathcal{I}$. Since $\mathcal{I}$ is compact and the function $H(u)$ and $h(u,\varrho)$ is continuous in u, the infimum is attained. Let u^* be the point in $\mathcal{I}$ which achieves the minimum of $H(u)$ and u^*_ϱ be the point in $\mathcal{I}$ which achieves the minimum of $h(u,\varrho)$. Then, for all $\varrho > N_\epsilon$,

$$H(u^*) \leq H(u^*_\varrho) < h(u^*_\varrho,\varrho) + \epsilon,$$
$$h(u^*_\varrho,\varrho) \leq h(u^*,\varrho) < H(u^*) + \epsilon.$$

These two sets of inequalities gives

$$|H(u^*) - h(u^*_\varrho,\varrho)| < \epsilon$$

for all $\varrho > \varrho_\epsilon$. Since this holds for every $\epsilon > 0$, the proposition is proved. ∎

Proposition 4.3 *Let $\mathcal{I} \subset \mathbb{R}$ be a closed bounded (and hence compact) interval. Then, for all $x \in \mathcal{I}$:*

$$\begin{aligned}\lim_{\varrho\to\infty} J^J_{(1,2,\varrho)}(x) &= \kappa^{1,J}_{(1,2)}x^2 + \kappa^{2,J}_{(1,2)}\sigma_w^2,\\ \lim_{\varrho\to\infty} J^C_{(1,2,\varrho)}(x) &= \kappa^{1,C}_{(1,2)}x^2 + \kappa^{2,C}_{(1,2)}\sigma_w^2,\end{aligned}$$

where the coefficients are given by (3.5) and (3.6).

Proof: Recall that $J^J_{(1,2,\varrho)}(x)$ is given by

$$J^J_{(1,2,\varrho)}(x) = x^2 + E\{V_{(0,1,\varrho)}(Ax+w)|I_0\}, \tag{4.11}$$

where

$$\begin{aligned}E\{V_{(0,1,\varrho)}(Ax+w)|I_0\} &= \int_{-2\varrho/A}^{2\varrho/A} V^1_{(0,1,\varrho)}(\tilde{x})f(\tilde{x}|x)d\tilde{x} + \int_{-\infty}^{-2\varrho/A} V^2_{(0,1,\varrho)}(\tilde{x})f(\tilde{x}|x)d\tilde{x}\\ &\quad + \int_{2\varrho/A}^{\infty} V^2_{(0,1,\varrho)}(\tilde{x})f(\tilde{x}|x)d\tilde{x},\end{aligned}$$

and $f(\tilde{x}|x) = \mathcal{N}(Ax, \sigma_w^2)$. As we take the limit $\varrho \to \infty$, we see that the second and third term in the expectation drop out. Then we are left with

$$\begin{aligned}E\{V_{(0,1,\varrho)}(Ax+w)|I_0\} &= \lim_{\varrho\to\infty}\int_{-2\varrho/A}^{2\varrho/A} V^1_{(0,1,\varrho)}(\tilde{x})f(\tilde{x}|x)d\tilde{x}\\ &= \left(1+\frac{A^2}{2}\right)\left(A^2x^2+\sigma_w^2\right)+\sigma_w^2.\end{aligned}$$

Substituting it back into (4.11), we get

$$\lim_{\varrho\to\infty} J^J_{(1,2,\varrho)}(x) = \left(1+A^2+\frac{A^4}{2}\right)x^2 + \left(2+\frac{A^2}{2}\right)\sigma_w^2,$$

which is the same as the cost for the unconstrained case given by (3.3). Next consider the case when the controller is active. The cost is given by

$$\lim_{\varrho\to\infty} J^C_{(1,2,\varrho)}(x) = \inf_u \left(\lim_{\varrho\to\infty} x^2 + u^2 + E\{V_{(1,1,\varrho)}(Ax+u+w)\}\right). \tag{4.12}$$

The expected value is

$$E\{V_{(1,1,\varrho)}(Ax+u+w)|I_0\} = \lim_{\varrho\to\infty}\int_{-\varrho/A}^{\varrho/A} V^1_{(1,1,\varrho)}(\tilde{x})f(\tilde{x}|x)d\tilde{x},$$

since the other terms drop out because of the interval of the integration is from ∞ to ∞. Here, $f(\tilde{x}|x) = \mathcal{N}(Ax+u, \sigma_w^2)$. Note that due to bounded interval of x, the control values are bounded and the function which we are minimizing has a pointwise uniform convergence as ϱ increases. Therefore, we can interchange

the limit and the infimum. Again, simplifying the equation gives

$$E\{V_{(1,1,\varrho)}(Ax+u+w)|I_0\} \quad = \quad (1+A^2)((Ax+u)^2+\sigma_w^2)+\sigma_w^2.$$

Since this is a quadratic function of u, the first derivative gives the optimal value of control action u, and it is

$$u^*_{(1,2)}(x) = -A\left(\frac{1+A^2}{2+A^2}\right)x.$$

Putting this optimal control value back in (4.12), we get

$$\lim_{\varrho\to\infty} J^C_{(1,2,\varrho)}(x) \quad = \quad \left(1+A^2-\frac{A^2}{2+A^2}\right)x^2+\left(2+A^2\right)\sigma_w^2.$$

This proves the proposition. The main technical step in this proof consists in guaranteeing that the "$\inf_u$" and "$\lim_{\varrho\to\infty}$" terms can be swapped in the computation of $\lim_{\varrho\to\infty} J^C_{(1,2,\varrho)}(x)$, for a fixed $x \in \mathcal{I}$. This follows directly from Propositions 4.1 and 4.2 proved above. ■

In the proposition above, we proved that as the constraint is relaxed, we recover the same cost function and value functions as in the game with unconstrained state. As a result of this, we also find that the threshold function for the jammer is same as that derived in (3.7) in Chapter 3.

Next, we prove a proposition which gives the lower threshold as a linear function of noise variance when the ratio ϱ/σ_w is a constant.

Proposition 4.4 *If $\varrho/\sigma_w = \upsilon$, then $\tau^c_{(1,2),l} = g(\upsilon, A)\sigma_w$ where $g(.)$ is satisfies*

$$\tilde{J}^J_{(1,2)}(g(\upsilon,A)) - \tilde{J}^C_{(1,2)}(g(\upsilon,A)) = 0. \tag{4.13}$$

The cost calculated above is for the system that has zero mean unit variance noise ($\sigma_w = 1$) and υ as its state constraint.

Proof: Let us transform our state variable x to $\xi := x/\sigma_w$. At first, we prove that if $\varrho/\sigma_w = \upsilon$, then the optimal control at $(1,2)$ is a linear function of σ_w. The optimal control value is

$$u^*_{(1,2)}(x) \quad = \quad \arg\min_u x^2+u^2+E\{V_{(1,1,\varrho)}(Ax+u+w)|I_0\}, \tag{4.14}$$

$$\quad = \quad \arg\min_u \sigma_w^2\left(\xi^2+\frac{u^2}{\sigma_w^2}+E\left\{V_{(1,1,\varrho)}\left(A\xi+\frac{u}{\sigma_w}+\frac{w}{\sigma_w}\right)|I_0\right\}\right). \tag{4.15}$$

Define $\tilde{u} := u/\sigma_w$, change the variable of integration to $\tilde{x} = x/\sigma_w$ and interval of integration, we get the minimizing function as

$$\tilde{u}^*_{(1,2)}(\xi) \quad = \quad \arg\min_{\tilde{u}}\left(\xi^2+\tilde{u}^2+E\left\{\tilde{V}_{(1,1)}\left(A\xi+\tilde{u}+\frac{w}{\sigma_w}\right)|I_0\right\}\right). \tag{4.16}$$

Here $\tilde{V}_{(1,1,\upsilon)}$ is the value function for the game with state constraint υ and unit noise variance. Minimizing with respect to u in (4.14) is the same as minimizing with respect to $\tilde{u}$ in (4.16). Now, the expression in (4.16) is independent of σ_w and ϱ, and is dependent only on the value of υ, A and ξ. Given the value of

$\tilde{u}^*_{(1,2)}(\xi)$, we transform the system back to the original game to get $u^*_{(1,2)}(x) = \tilde{u}^*_{(1,2)}(\xi)\sigma_w$. Therefore, the optimal control is a linear function in σ_w.

Let us consider the difference in the cost with jamming and the cost with controlling. It is given by

$$J^J_{(1,2,\varrho)}(x) - J^C_{(1,2,\varrho)}(x) = E\{V_{(0,1,\varrho)}(Ax+w)|I_0\} - u^{*2}_{(1,2)}(x) - E\{V_{(1,1,\varrho)}(Ax+u^*_{(1,2)}(x)+w)|I_0\}.$$

Again, applying the transformation and changing the limits in the integration terms appropriately, we get this difference as

$$J^J_{(1,2,\varrho)}(x) - J^C_{(1,2,\varrho)}(x) = \sigma_w^2 \left(\tilde{J}^J_{(1,2,\upsilon)}(\xi) - \tilde{J}^C_{(1,2,\upsilon)}(\xi)\right). \tag{4.17}$$

By definition, lower threshold $\tau^c_{(1,2),l}$ is defined as the value where the difference in the cost with jamming is equal to the cost with control, i.e. it is a zero of (4.17). The zero of the right hand side of (4.17) is $g(\upsilon, A)$. Using this fact and transforming the system back to $x = \xi\sigma_w$, we complete the proof of the proposition. ∎

In the proposition above, we have seen that for a system with a given A, the threshold is a constant dependent on the ratio ϱ/σ_w multiplied with the noise variance σ_w. System designers can use this result to get an acceptable value of the constraint ϱ as a function of the noise variance σ_w.

4.4 Numerical Simulations

In this section, we discuss some simulation results which we obtained for various values of the parameters A, ϱ and σ_w. The results obtained are for $x \geq 0$, but similar results hold for $x < 0$ also. We have normalized our x-axis to be equal to Ax/ϱ, so that the jammer is active only when $Ax/\varrho \leq 1$. All simulations were performed in MATLAB. Integration of value functions were performed using the standard `ode45` function of MATLAB. Since the integration can not be performed till ∞, the upper limit of integration was taken to be $|Ax+u| + 2\varrho/A + 10\sigma_w$ (and lower limit was $-(|Ax+u| + 2\varrho/A + 10\sigma_w)$). The maximum step size for integration was limited to $5\sigma_w$ to achieve desired accuracy. For calculating the infimum of the cost function, differentiation was performed numerically and `fzero` function was invoked to find the infimum. Lower threshold was calculated by interpolating the cost function between two values of state x_1 and x_2 at which $J^C_{(1,2,\varrho)}(x_1) > J^J_{(1,2,\varrho)}(x_1)$ and $J^C_{(1,2,\varrho)}(x_2) < J^J_{(1,2,\varrho)}(x_2)$ to find the point where the two costs are equal $J^C_{(1,2,\varrho)}(\tau^c_{(1,2)l}) = J^J_{(1,2,\varrho)}(\tau^c_{(1,2)l})$.

In Figure 4.1, we see that when the state is small, the actuator noise on the system in this stage will increase the state of the system. Therefore it is optimal for the jammer to jam at the next step. This is the reason why we see that the jammer's optimal policy requires the jammer to not jam when the state is small. After the lower threshold, the cost function with jamming is always higher than the cost function with control. Hence, the jammer jams up to $x \leq \varrho/A$ and after that the state constraint becomes active and the jammer cannot jam the channel.

In Figure 4.2, we notice that the lower threshold for the jammer in the constrained case is always lower than the threshold for the unconstrained case. In the unconstrained game, the jammer's policy is to jam when the state x is above that threshold. However, in the constrained case, the jammer is forced to reduce the lower threshold in order to satisfy the state constraint, as well as increase the cost to the controller

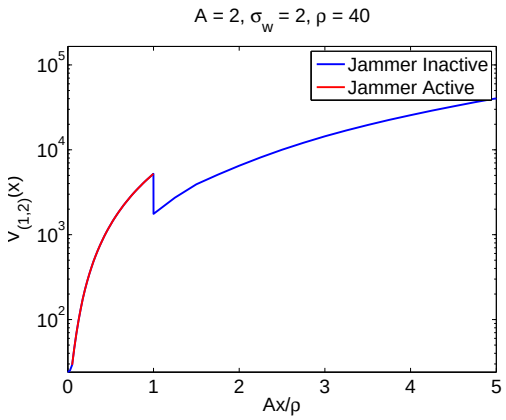


Figure 4.1: The value function at stage $(1,2)$ with state constraint parameter $\varrho = 40$ and system parameters $A = 2$ and $\sigma_w = 2$. The red region denotes the values of x, where the jammer jams.

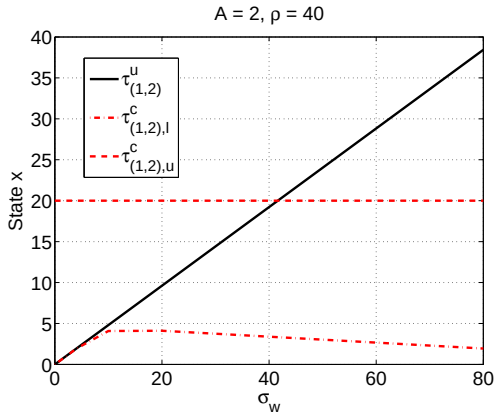
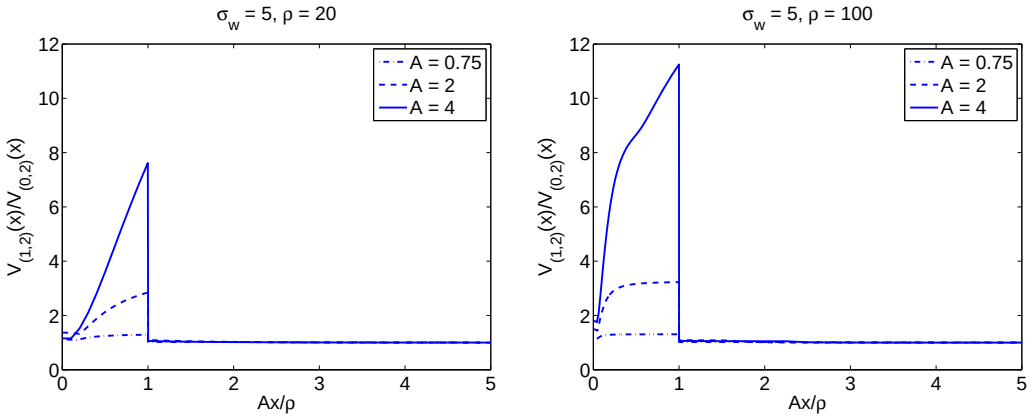


Figure 4.2: The threshold variation as a function of σ_w. Here, superscript u denote threshold for unconstrained game considered in Chapter 3 and superscript c denotes threshold for constrained game. The region between dotted lines is the region where jamming is optimal at stage $(1,2)$ for the constrained game.

strategically. We also see that when the threshold for the unconstrained game $\tau_{(1,2)}$ is much smaller than the upper threshold for the constrained game $\tau^c_{(1,2),u} := \varrho/A$ (this happens when σ_w is small), the lower threshold curve overlaps the threshold curve for the unconstrained game. This is due to the fact that the tail of the Gaussian probability distribution goes to zero very rapidly for small σ_w. This reduces the effect of state constraint when state and noise variance is small. Also, as the noise variance becomes larger, the lower threshold reduces to zero.

In Figure 4.3, we compare the increase in cost the system suffers due to the action of jammer. We plot the ratio of value function for stage $(1,2)$ and stage $(0,2)$ in this figure. At stage $(0,2)$, the jammer has no chance left to jam till the end of the horizon. Therefore, the value function is the optimal cost for constrained optimization (note that the state constraint is still active). For the same noise variance, we see that the presence of the jammer inflicts higher cost to the unstable system if the constraint is relaxed. Notice that for $A = 4$, $\varrho = 100$ has a value function ratio exceeding 11 while for $\varrho = 20$, the ratio is less than 8. Therefore, if the system is unstable and the jammer is present, the designer should try to keep the state constraint as

small as possible.



(a) (b)

Figure 4.3: The ratio of value function with a jammer and without a jammer with state constraint active in both cases.

The case of $M \geq 2$ and for a general state space can also be solved using the techniques discussed in this chapter. However, the exact calculation of the set of states when the jammer jams is difficult to obtain. For the case when $M \geq 2$, we need to calculate the threshold for all the nodes which is in the path from (M, N) to $(0, 0)$ in the tree given in Figure 2.2. In the multi-dimensional case, it is not hard to see that the expectation value of the value functions at the next stage would require integration in n-dimension. Also, instead of thresholds that we get for the scalar case, we get hyperplanes separating the region where the jammer is active and where the controller is active.

Therefore, computation of saddle-point strategy for general cases requires significant computational effort even for simple games. If M is large, or the state dimension is large, then obtaining the accurate strategy for the jammer and the controller is very difficult from a computational perspective. Therefore, one must switch to approximation schemes in order to compute the saddle-point equilibrium strategy for the controller and the jammer. However, intuitively, the jammer would jam if the state is "large" but below the upper threshold and not jam if the state is "small". It is the intermediate values of state where the jammer needs to know the exact values of thresholds (or hypersurfaces in case of multi dimensional state space) to have strategic advantage.

In this chapter, we assumed that the communication channel can transmit control signal in the form of an analog signal, which can send real numbers. Also, jamming is assumed to completely block the control signal. However, in digital systems, the control signal (and observation signal) needs to be quantized and the quantized signal is encoded into bits, which are then sent across the communication channel. We treat a class of jamming attacks in such systems, where instead of blocking the signal completely, the jammer flips limited number of bits in the encoded signal.

CHAPTER 5

ONE STEP CONTROL WITH FINITE CODELENGTH

We consider in this chapter a type of deception attack on a control system, where a jammer flips a limited number of bits in the observation signal, which is assumed to be of finite codelength. However, to gain insight into the problem and for simplicity of exposition, we restrict our attention to a noisy scalar system playing a static game with the jammer. We provide precise problem formulation in Section 5.1. In Section 5.2, we restrict our attention to binning based control strategy for the controller in order to obtain an upper bound on the minimum cost that the controller incurs due to the presence of the jammer. We also discuss relevant tools from error correcting coding theory for the problem in this section. In the Section 5.3, we explore the theory of rate distortion from information theory to arrive at the ultimate lower bound on the codelength that is required to keep the state bounded. We provide some concluding remarks in Section 5.4. The results discussed in this chapter have been reported in [36].

5.1 Problem Formulation

Using scalar system dynamics, the scenario can be captured through the following mathematical formulation: The state equation evolves as (note that we have one stage problem)

$$x^+ = Ax + u + w, \tag{5.1}$$

where $x, x^+ \in \mathbb{R}$ is the state of the plant, $u \in \mathbb{R}$ is the control signal, w is a discrete-time zero mean uniformly distributed random variable with bound Δ (i.e. $w \sim \mathscr{U}(-\Delta, \Delta)$). Initial state x is also a zero mean uniformly distributed random variable in the interval $\mathcal{I} := [-1, 1]$ and independent of process noise w.

What we consider is a prototype of a scenario where the controller and the plant are far from each other, such that the plant sends the state information to the controller and the controller sends the control signal to the plant via a communication channel. For the analysis, the channel is assumed to be perfect (but unsecured) and it does not induce any error on the received bit at the controller or the plant end (only jammer can induce errors). The plant and the controller can send at most n bits across the channel. The signal sent over the channel from the plant to the controller is intercepted by a jammer, which can flip at most t bits of the codewords of the observation signal. We assume that the jammer jams the channel from the plant to the controller, while the channel from the controller to the plant is not intercepted by the jammer. We refer to n as the channel rate[1] in this chapter.

Figure 5.1 provides a schematic description of the interconnections and the flow of information in the

[1]Note that this definition of channel rate differs from the usual meaning of channel rate in information theory.

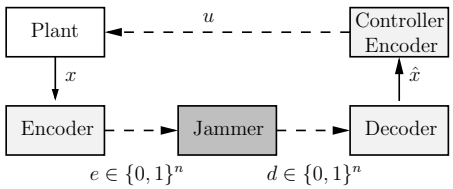


Figure 5.1: Control in the presence of an intelligent jammer. The lightly shaded blocks belong to one player (referred to as controller) and the darker shaded block is the other player (the jammer). See text for details.

system. The dotted lines denote wireless channel which is susceptible to jamming attacks and the solid lines are physical wires transferring information from one subsystem to another and is assumed to be secured.

In the problem described above, it is desired that the plant does not deviate too much from a desirable point. Hence, if the state of the system starts within a bounded set, we would like the state at the next time instant to remain bounded (in the same set) with high probability. Thus, the cost function associated with this problem is

$$J = P\left\{x^+ \notin \mathcal{I} | x \in \mathcal{I}\right\} \tag{5.2}$$

which is to be minimized by the encoder-decoder-controller team and maximized by the jammer. Notice that the three players (controller, encoder and the decoder) act as a team for this problem, though the information feeding into each player of the team is different. We will henceforth refer to this team as controller, while in fact, it comprises three players.

For a given channel rate $n > 0$ and jamming parameter $t \geq 0$, we denote by $\mathcal{E}_n$ the set of all measurable maps from $\mathcal{I}$ to $\{0,1\}^n$, by $\mathcal{J}_{(t,n)}$ the set of all maps from $\{0,1\}^n$ to $\{0,1\}^n$ with Hamming distortion less than or equal to t, and by $\mathcal{D}_n$ the set of all maps from $\{0,1\}^n$ to $\mathbb{R}$. The set $\mathcal{E}_n \times \mathcal{D}_n$ can be thought of as the strategy space for the team composed of the encoder, which communicates the plant's observation in n bits, and the decoder/controller, which maps the possibly corrupted message at the end of the channel into a control input. Similarly, $\mathcal{J}_{(t,n)}$ is the jammer's strategy space, which flips at most t bits in the encoded sequence. To every choice $(e,d) \in \mathcal{E}_n \times \mathcal{D}_n$ of the encoder-decoder/controller team and $j \in \mathcal{J}_{(t,n)}$ of the jammer corresponds the cost $J(x, d(j(e(x))))$ which, by a slight abuse of notation, we denote by $J(e,d;j)$.

We are interested in computing

$$\gamma(n) := \inf_{(e,d)\in\mathcal{E}_n\times\mathcal{D}_n} \sup_{j\in\mathcal{J}_{(t,n)}} J(e,d;j) \tag{5.3}$$

as a function of the channel rate n and, in particular, in determining the smallest rate $n^\star$ for which $\gamma(n) = 0$ for all $n \geq n^\star$.

We start by providing an upper bound for $\gamma(n)$ by restricting the encoder-decoder/controller team's strategy space to binning-based policies that respect a separation principle. This also yields an upper bound for $n^\star$. Then, in Section 5.3, we use rate distortion theory to compute a lower bound for $n^\star$, which is within a multiplicative constant from the Hamming bound.

5.2 Binning Based Strategies and an Upper Bound

Intuitively, when there is finite length encoding of a real number, the most obvious solution strategy is to use quantization and binning based strategy for the controller. The interval $\mathcal{I}$ is divided into N intervals (henceforth, termed as bins). The encoder takes x as the input, determines which bin x belongs to, and outputs the codeword corresponding to that bin. Therefore, we force the controller to use a binning based strategy, which naturally restricts encoding strategies to code and send the bin index across the channel. Note that our problem formulation in the previous section does not enforce this structure on the controller. This specific solution strategy is chosen to find a constructive upper bound on $\gamma(n)$ as defined in the previous section and an upper bound on the number of bits n required to drive the cost to zero.

We consider the case for $A > 1$, since for $|A| \leq 1$, a trivial control strategy is to use *zero*. The case of $A < -1$ yields the same value with A replaced by $|A|$.

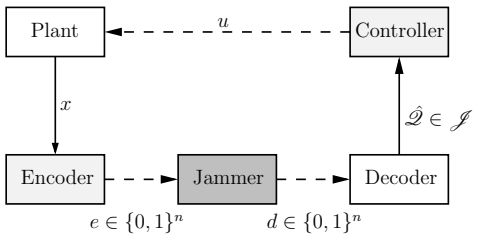


Figure 5.2: The binning based strategy in the presence of a jammer.

The flow of information in the system is as follows (see Figure 5.2). The state information x of the plant is sent to the encoder, which encodes the bin index corresponding to the state into $e \in \{0,1\}^n$. The jammer flips at most t bits in this sequence to produce $d \in \{0,1\}^n$. The decoder at the controller end receives this jammed sequence d and determines which bin index $\hat{\mathscr{Q}}$ this sequence belongs to using nearest neighbor search. This information is then used by the controller to compute the control value for the plant and the index corresponding to the control value is sent to the plant over the communication channel. Therefore, in this scenario, the three players (encoder, decoder and controller) act as a team (collectively called the controller) and the jammer acts as the fourth player. The codeword associated with each bin index and the codeword associated with each control action is known to everyone, including the jammer.

5.2.1 Notation

In order to obtain an upper bound on $\gamma(n)$ under the restriction of using binning based control strategy, we need to introduce some additional notation. Let $H(\cdot,\cdot)$ denote the Hamming distance [37] between two codewords. We say that an encoding strategy $e \in \mathcal{E}_n$ is N bin-based if there exists a partition $(\mathcal{B}_1, ..., \mathcal{B}_N)$ of the interval $\mathcal{I}$ such that

$$\mathcal{I} = \bigcup_{i \in \mathscr{J}} \mathcal{B}_i$$

and corresponding to each bin $\mathcal{B}_i$, there exists a codeword $\epsilon_i \in \{0,1\}^n$ such that

$$e(x) \quad = \quad \epsilon_i \text{ for all } x \in \mathcal{B}_i.$$

If, in addition, the codewords satisfy

$$H(\epsilon_i, \epsilon_k) \geq 2s+1 \text{ for all } i \neq k, \quad s \in \mathbb{N} \cup \{0\}, \tag{5.4}$$

we say that the encoding strategy $\mathcal{E}_n$ is s-error free. Let $\epsilon \in \{0,1\}^n$ be the codeword received by the decoder and define $h(\epsilon)$ by the following relation:

$$h(\epsilon) := \underset{i \in \mathscr{J}}{\arg\min} \; H(\epsilon_i, \epsilon). \tag{5.5}$$

We will denote $h(\epsilon)$ by $\hat{\mathscr{Q}}$ which lies in the set $\mathscr{J}$. We say that a decoding strategy $d \in \mathcal{D}_n$ is N bin-based if there exist N codewords $\epsilon_i \in \{0,1\}^n$ ($i \in \mathscr{J}$) and N control inputs $u_1, ..., u_N \in \mathbb{R}$ such that

$$d(\epsilon) = u_{h(\epsilon)} \text{ for all } \epsilon \in \{0,1\}^n.$$

The set of points $\mathcal{T}_i \subset \mathcal{I}$ where the control u_i keeps the state within the interval $\mathcal{I}$ is given by

$$\mathcal{T}_i = \left[\frac{-1+\Delta-u_i}{A}, \frac{1-\Delta-u_i}{A} \right] \cap \mathcal{I}. \tag{5.6}$$

We define $\mathscr{N}_i \subseteq \mathscr{J}$ as the set of bin indices whose codewords are less than or equal to $2t$ Hamming distance away from the codeword for bin i :

$$\mathscr{N}_i = \{k \in \mathscr{J} : k = h(j(e(x))), \; x \in \mathcal{B}_i, \; j \in \mathcal{J}_{(t,n)}\}, \tag{5.7}$$

where $h(\cdot)$ is defined in (5.5). Clearly, the set $\mathscr{N}_i$ for each bin index $i \in \mathscr{J}$ is dependent on the encoding strategy. Since the jammer flips at most t bits, the set $\mathscr{N}_i$ consists of all bin indices corresponding to the nearest neighbors of all 0 to t flips in the codeword for i^{th} bin. Denote $p_{ik}, \; k \in \mathscr{N}_i$ to be the probability with which the jammer flips the bits in the codeword corresponding to i^{th} bin such that the resulting codeword corresponds to the codeword of the k^{th} bin.

We say that N bin-based encoding and decoding strategies are adapted if the codewords $\{\epsilon_1, ..., \epsilon_N\}$ are the same for both strategies, and refer to the pair (e, d) as s-error free. The set of all adapted N bin-based, s-error free encoding and decoding strategy pairs with codelength n is denoted by $\mathcal{S}_{(n,N,s)}$.

Although an N bin-based decoding strategy may not be well-defined over $\{0,1\}^n$ (because there may be more than one index satisfying (5.5)), the expression $d(j(e(x)))$ is well defined for every $x \in \mathcal{I}$, every N bin-based encoding strategy *e that is adapted to d and t-error free*, and every $j \in \mathcal{J}_{(t,n)}$. Indeed, in this case, condition (5.4) ensures that every codeword used by the encoding and decoding strategies is uniquely recovered by the nearest neighbor rule (5.5), regardless of which t out of its n bits are flipped. In addition, for every $(e, d) \in \mathcal{S}_{(n,N,t)}$,

$$d(j(e(x))) = u_i \; \Leftrightarrow \; x \in \mathcal{B}_i$$

for all $j \in \mathcal{J}_{(t,n)}$ and all $x \in \mathcal{I}$.

In words, when the encoder-decoder/controller team uses a pair of strategies in $\mathcal{S}_{(n,N,t)}$, it is guaranteed that system (5.1) will receive the input signal corresponding to the actual bin in which the state lies, regardless of the action of the jammer. The goal of the team is to achieve a cost $\sup_{j\in\mathcal{J}_{(t,n)}} J(e,d;j)$ of zero by appropriately choosing control inputs corresponding to each bin.

It is clear that for all $(e,d) \in \mathcal{S}_{(n,N,t)}$ and all $j \in \mathcal{J}_{(t,n)}$

$$\gamma(n) \leq \inf_{(e,d)\in\mathcal{S}_{(n,N,t)}} \sup_{j\in\mathcal{J}_{(t,n)}} J(e,d;j),$$

since we are restricting the strategy space of the controller to binning-based control strategies.

The following result, which is classical in the theory of error correcting codes, provides conditions for the (non) existence of s-error free N bin based encoding strategies.

Lemma 5.1 (Gilbert & Hamming bounds [37]) *If*

$$N \leq \frac{2^n}{\sum_{j=0}^{2t} \left(\begin{array}{c} n \\ j \end{array} \right)}, \tag{5.8}$$

then there exists a t-error free N bin-based encoding strategy. However, if

$$N > \frac{2^n}{\sum_{j=0}^{t} \left(\begin{array}{c} n \\ j \end{array} \right)}, \tag{5.9}$$

there does not exist a t-error free N bin-based encoding strategy.

Lemma 5.1 implies that, for every N and t, the set of all rates n for which there exists a t-error free N bin based encoding strategy is non-empty. In addition, its minimal element, denoted by $n_{ecc}(N,t)$, satisfies

$$n_{Hamming}(N,t) \leq n_{ecc}(N,t) \leq n_{Gilbert}(N,t), \tag{5.10}$$

where $n_{Hamming}(N,t)$ and $n_{Gilbert}(N,t)$ are given by

$$\begin{aligned} n_{Hamming}(N,t) &= 1 + \max \left\{ n \in \mathbb{N} : N > \frac{2^n}{\sum_{j=0}^{t} \left(\begin{array}{c} n \\ j \end{array} \right)} \right\} \\ n_{Gilbert}(N,t) &= \min \left\{ n \in \mathbb{N} : N \leq \frac{2^n}{\sum_{j=0}^{2t} \left(\begin{array}{c} n \\ j \end{array} \right)} \right\} \end{aligned}$$

Hence, an upper bound on the value of $\gamma(n)$ can be obtained by considering a zero-sum game between the jammer and encoder-decoder/controller team, with the strategy space of the latter restricted to $\mathcal{S}_{(n,N,t)}$.

5.2.2 Control Without Jammer

We consider the case without a jammer and obtain a binning and control strategy. The main purpose of the Lemma below is to come up with a necessary condition on the number of bins which are required to keep the state bounded in the next time step.

Lemma 5.2 *Let n, N, and t be such that N bin-based, t-error free encoding strategies exist. Then there exist $(\bar{e}, \bar{d}) \in \mathcal{S}_{(n,N,t)}$ such that $J(\bar{e}, \bar{d}; j) = 0$ for all $j \in \mathcal{J}_{(t,n)}$ if and only if*

$$N \geq \left\lceil \frac{|A|}{1-\Delta} \right\rceil. \tag{5.11}$$

In addition, when (5.11) holds, $\bar{e}$ and $\bar{d}$ can be constructed with the following choice of bins $(\mathcal{B}_1, ..., \mathcal{B}_N)$ and control inputs $u_1, ..., u_N$:

- *if N is odd:*

$$\mathcal{B}_k = \left[\frac{2k-1}{N}, \frac{2k+1}{N} \right), \; u_k = -\frac{2kA}{N}, \tag{5.12}$$

  for all $-\frac{N-1}{2} \leq k \leq \frac{N-1}{2}$

- *if N is even,*

$$\mathcal{B}_k = \left[\frac{2(k-1)}{N}, \frac{2k}{N} \right), \; u_k = -\frac{(2k-1)A}{N}, \tag{5.13}$$

  for all $-\frac{N}{2} + 1 \leq k \leq \frac{N}{2}$.

In both cases, any set of codewords $\epsilon_1, ..., \epsilon_N \in \{0,1\}^n$ which renders $\bar{e}$ t-error free can be chosen.

Proof: Let there exist $(\bar{e}, \bar{d}) \in \mathcal{S}_{(n,N,t)}$ such that $J(\bar{e}, \bar{d}; j) = 0$. Consider a bin $\mathcal{B}_i$, $x_1 := \inf \mathcal{B}_i$, $x_2 := \sup \mathcal{B}_i$ and assume the control for this bin to be u and $A > 0$. Since the state at the next step is bounded, we need the following to hold:

$$\begin{aligned} Ax_1 + u &\geq -1 + \Delta \\ Ax_2 + u &\leq 1 - \Delta. \end{aligned}$$

Subtracting the first from the second, we get $x_2 - x_1 \leq \frac{2(1-\Delta)}{A}$. Hence, the maximum bin size cannot be greater than $2(1-\Delta)/A$ in order to keep the state bounded. The number of bins N required to cover the interval $\mathcal{I}$ is $\lceil 2/(2(1-\Delta)/A) \rceil = \left\lceil \frac{A}{1-\Delta} \right\rceil$. Again, the result for negative values of A can be obtained using similar steps.

If $N = \left\lceil \frac{|A|}{1-\Delta} \right\rceil$, then the binning and control strategy given by (5.12) for odd N and (5.13) for even N in the lemma above keeps the state in the interval.

Substituting the control value u_k for x corresponding to bin $\mathcal{B}_k$ keeps the state within the interval $\mathcal{I}$. Note that this control strategy works for equispaced bins only. ∎

When noise is not present in the system, then $\Delta = 0$. The length of codeword in this case is $\log_2 \lceil |A| \rceil$. The result is not surprising, since it has been shown in [1, 2, 3] that the channel rate has to be (strictly)

greater than $\log_2 |A|$ for the system to be stabilizable. Although our goal here is a little different (the state has to remain in the interval $\mathcal{I}$ instead of stabilizable), the results are essentially the same (without the strict inequality) as those obtained in these references. This is, however, not true for a system which has bounded noise as shown in the Lemma above.

If the noise is unbounded (as in the case of Gaussian process noise), then there is no control strategy with the finite channel rate scheme which can keep the state within the given bound with probability 1.

The essence of the results in this section is that there are certain minimum number of bins required (as proved in Lemma 5.2) for the system state to remain in the same interval in the next time step. This number of bins are dependent of the system parameter A and the maximum magnitude of noise Δ. Now, we are prepared to consider the problem with the jammer in the next subsection.

5.2.3 Jamming and Error Correcting Code

In Lemma 5.2, we noticed that a certain minimum number of bins is necessary for the controller to be able to keep the state bounded even without a jammer. If the number of bins is less than that, then there is no hope of being able to keep the state within the interval $\mathcal{I}$ in the next time step. The number of bits that are required to send codewords for N bins is $\lceil \log_2(N) \rceil$.

In the presence of a jammer which can flip at most t bits, the codelength n above which the errors can be corrected is bounded below by the Hamming bound and above by the Gilbert bound [37] (see Lemma 5.1). Establishing the Hamming and Gilbert bounds do not involve a constructive proof and rely on random coding strategy for constructing codewords. Recall that the minimum n for which t errors can be corrected by decoder for the N bin case is $n_{ecc}(N,t)$. It is clear from (5.10) that $n_{ecc}(N,t)$ lies between the Hamming bound and the Gilbert bound. However, currently, it is not known how close $n_{ecc}(N,t)$ is to the Hamming bound or the Gilbert bound [37]. There are only a few coding strategies for which the Hamming bound is tight, and they are known as perfect codes [37].

It is clear that the number of bits required for the specific number of bins is going to be much larger than $\log_2(N)$ in the presence of the jammer. Therefore, when the channel rate $n < n_{ecc}(N,t)$ but $n \geq \log_2(N)$, then the only way to design the control strategy is by computing saddle-point equilibrium strategy for the zero-sum game between the controller and the jammer. Towards this end, we need to compute $(e^*, d^*) \in \mathcal{E}_n \times \mathcal{D}_n$ and $j^* \in \mathcal{J}_{(t,n)}$ such that

$$J(e^*, d^*; j) \leq J(e^*, d^*; j^*) \leq J(e, d; j^*),$$

which holds for all $(e,d) \in \mathcal{E}_n \times \mathcal{D}_n$ and $j \in \mathcal{J}_{(t,n)}$. This means that the binning, encoding and control strategies have to be chosen intelligently to mitigate the adverse effect of jamming. This is addressed in next subsection. Figure 5.3 shows the various regions where each solution concept works for this class of problems. In the figure, n_{ecc} is the minimum channel rate at which t-flips in the codewords can be corrected for N bins by using an appropriate error correcting algorithm.

In the following theorem, we present a sufficient condition on the channel rate n, such that the error correction coding technique can be applied to the problem so as to mitigate the error resulting due to the adversarial action by the jammer. Since the proof is constructive, we also obtain a coding scheme and a decoding scheme which achieve this bound.

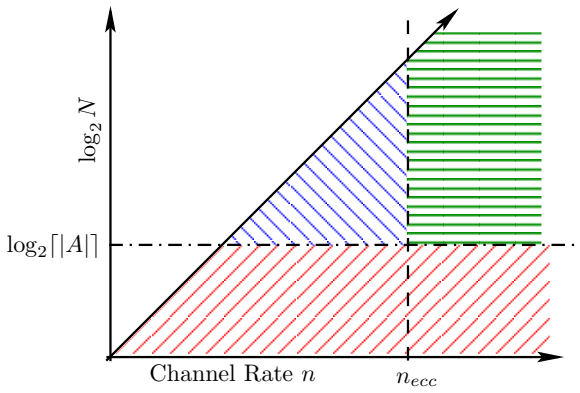


Figure 5.3: The graph shows the region on channel rate n - $\log_2 N$ plot where the state cannot be guaranteed to be within a given bound with probability 1 (red region), saddle-point equilibrium may achieve a better performance than the worst case (blue region), and where the jammer is ineffective (green region) due to error correcting coding algorithms.

Theorem 5.3 *Let N be the number of bins and n be the codelength, and assume that the jammer can flip at most t bits. Then, a sufficient condition on the codelength n for the jammer to have no effect on the control signal is*

$$n \geq t n_{cr} + \lceil \log_2 N \rceil \,, \tag{5.14}$$

where $n_{cr} \in \mathbb{N}$ satisfies

$$n_{cr} = \min \left\{ n \in \mathbb{N} : N \leq \begin{pmatrix} n \\ 0 \end{pmatrix} + \begin{pmatrix} n-1 \\ 1 \end{pmatrix} + \cdots + \begin{pmatrix} \lceil n/2 \rceil \\ \lfloor n/2 \rfloor \end{pmatrix} \right\}.$$

Proof: If two different codewords are sent and the jammer has flipped t bits in the codewords, then to be able to decode it without error, the two codewords should be $2t+1$ bit apart. With this idea, we now construct a set of codewords, such that the difference between any two codewords is of 2 bits. After this is done, we will extend the algorithm to $2t+1$ bit case by padding it with another set of codewords.

Let us suppose that n_{cr} number of bits are required to have a difference of 2 bits in any two codewords. Assume first codeword to be 000...(n_{cr} times). Now fix the first bit in the codeword to be 1 and put 1 at any of the $n_{cr}-1$ places. There are $\begin{pmatrix} n_{cr}-1 \\ 1 \end{pmatrix}$ ways of doing this. Then the difference between any two codewords is 2. Now, fix the first two bits to 1 and put two 1's at the remaining of the $n_{cr}-2$ places. There are $\begin{pmatrix} n_{cr}-2 \\ 2 \end{pmatrix}$ ways of doing this. Repeat this process until all the first $\lfloor n_{cr}/2 \rfloor$ bits are fixed to 1 and the rest of the $\lceil n_{cr}/2 \rceil$ bits have a combination of $\lfloor n_{cr}/2 \rfloor$ number of 1's. This way, we constructed the codewords for N bins and any two codewords in the set have a minimum distance of 2 bits. If the number of codewords required to control the plant reliably is N, then n_{cr} must satisfy

$$N \leq \begin{pmatrix} n_{cr} \\ 0 \end{pmatrix} + \begin{pmatrix} n_{cr}-1 \\ 1 \end{pmatrix} + \ldots + \begin{pmatrix} \lceil n_{cr}/2 \rceil \\ \lfloor n_{cr}/2 \rfloor \end{pmatrix}.$$

If the jammer has the ability to flip t bits, then we can replace each 0 in the codeword with a sequence of t 0's and 1 with a sequence of t 1's. This keeps the codewords a minimum of $2t$ bits apart.

Now "pad" the i^{th} codeword with the binary expansion of integer i. This will ensure that each of the two codewords have an additional distance of 1. This will require $\lceil \log_2 N \rceil$ number of additional bits. Summing the two expressions, we get the inequality in (5.14). ■

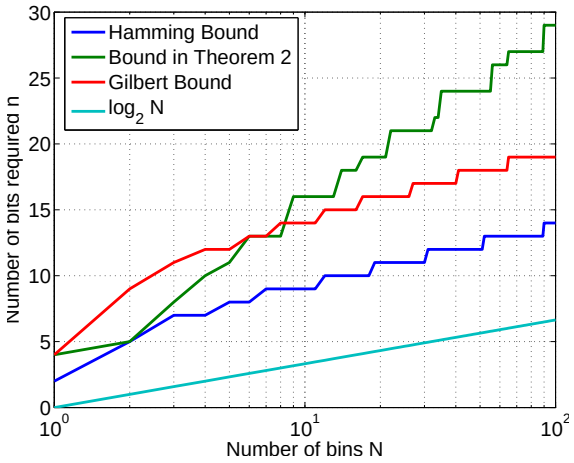


Figure 5.4: Various bounds on the channel rate when the jammer can flip at most $t = 2$ bits in codeword.

In Figure 5.4, we see the performance of the coding strategy in Theorem 5.3 with the Hamming bound and the Gilbert bound [37]. We notice that for up to $N = 8$ bins, our coding strategy is within the Hamming and Gilbert bounds. After that, the codelength of our coding strategy exceeds the Gilbert bound. Therefore, the coding scheme given by Theorem 5.3 can be improved to obtain a codelength below the Gilbert bound.

When the channel rate $n \geq n_{ecc}(N,t)$, then we can separately design the quantization, encoding and control policies. In that case, N bins (where N is given by Lemma 5.2) can be designed such that the information of the bin is reconstructed exactly at the controller end and it can send the correct control signal. The encoder is free to choose its policy independent of the control policy[2]. The cost in this case is *zero*, that is, the state will remain in the set $\mathcal{I}$ with probability 1. The following Theorem summarizes the result and provides a sufficient condition on rate n for which the cost is zero.

Theorem 5.4 *For the problem formulated in section 5.1 with binning-based control strategy, let there be* $N = \left\lceil \frac{|A|}{1-\Delta} \right\rceil$ *bins and the jammer can flip at most t bits. Then, the value of the game is zero if* $n \geq n_{ecc}(N,t)$, *i.e.,*

$$\gamma(n) = 0, \text{ for all } n \geq n_{ecc}(N,t).$$

As a result, we get $n^\star \leq n_{ecc}(N,t)$.

Proof: If $n \geq n_{ecc}(N,t)$, then there is an encoding policy with N codewords such that any pair of codewords have a Hamming distance greater than or equal to $2t+1$. From Lemma 5.2, we know that if

[2]The depenence of encoding policy on the control policy is addressed in the next subsection, where we consider the game scenario.

$N = \left\lceil \frac{|A|}{1-\Delta} \right\rceil$ and $n \geq n_{ecc}(N,t)$, then there exists $(\bar{e}, \bar{d}) \in \mathcal{S}_{(n,N,t)}$ such that $J(\bar{e}, \bar{d}; j) = 0$ for all $j \in \mathcal{J}_{(t,n)}$. Then, the policy given in Lemma 5.2 controls the plant such that the state remains in the interval $\mathcal{I}$ in the next time step. Hence, we achieve a value of *zero* for all jamming strategies. This results in $\gamma(n) = 0$ for all $n \geq n_{ecc}(N,t)$. ∎

If $n < n_{ecc}(N,t)$, then there is no encoding-decoding strategy which can correct all t flips by the jammer. Hence, there will always be "confusion" in a few bin indices sent by the encoder at the decoder's end. Using nearest neighbor search, the decoder may obtain wrong bin index, and hence, wrong control input is sent to the plant. Thus, the value of *zero* cannot be achieved by binning-based control strategy if $n < n_{ecc}(N,t)$.

Until now, we fixed the number of bins N and number of flips t to get the required channel rate n for zero cost. However, a more practical scenario is the one where the number of bits that can be transferred across a channel is limited by n. Therefore, we look into the case when channel rate $n < n_{ecc}(N,t)$ now. To do this, we need the following lemma which simplifies the cost function to make it easier to analyze.

Lemma 5.5 *The cost function of the game for the binning based control strategy is equivalent to*

$$P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{I} \right\} = \sum_{i=1}^{N} \sum_{k \in \mathcal{N}_i} p_{ik} P\{x \in \mathcal{B}_i \cap \mathcal{T}_k'\},$$

with the constraint $p_{ik} \geq 0$ *and*

$$\sum_{k \in \mathcal{N}_i} p_{ik} = 1, \forall\, i \in \{1, 2, ..., N\},$$

where $\mathcal{N}_i$ *and* $\mathcal{T}_i$ *is defined for all* $i \in \mathscr{J}$ *in (5.7) and (5.6) respectively.*

Proof: Using Bayes' theorem repeatedly, we can write the cost function as

$$P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{I} \right\} = \sum_{i=1}^{N} P\left\{ x \in \mathcal{B}_i \middle| x \in \mathcal{I} \right\} \left(\sum_{k \in \mathcal{N}_i} p_{ik} P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{B}_i, \hat{\mathscr{Q}} = k \right\} \right),$$

where $p_{ik} = P\left\{ \hat{\mathscr{Q}} = k \middle| x \in \mathcal{B}_i \right\}$ for all $k \in \mathcal{N}_i$ with the constraint

$$\sum_{k \in \mathcal{N}_i} p_{ik} = 1, \tag{5.15}$$

and $\hat{\mathscr{Q}} = h(j(e(x)))$. Now, recall the following identities

$$\begin{aligned} P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{B}_i, \hat{\mathscr{Q}} = k \right\} &= \frac{P\{x \in \mathcal{B}_i \cap \mathcal{T}_k'\}}{P\{x \in \mathcal{B}_i\}}, \\ P\left\{ x \in \mathcal{B}_i \middle| x \in \mathcal{I} \right\} &= P\{x \in \mathcal{B}_i\}. \end{aligned}$$

Using these expressions, the cost function is rewritten as

$$P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{I} \right\} = \sum_{i=1}^{N} \sum_{k \in \mathcal{N}_i} p_{ik} P\{x \in \mathcal{B}_i \cap \mathcal{T}_k'\}.$$

■

Next, we fix the rate n and the number of flips t, and define N_{cr} to be

$$N_{cr} = \max\{N \in \mathbb{N} : n \geq n_{ecc}(N, t)\}. \tag{5.16}$$

In this case, we can obtain N_{cr} number of codewords, each of codelength n, which are $2t+1$ bits apart. Using these set of codewords, we can obtain an upper bound on the cost function and as a consequence, an upper bound on $\gamma(n)$. Following theorem establishes an upper bound on the cost as a function of n.

Theorem 5.6 *Let N_{cr} be given by (5.16). If $N_{cr} < \lceil |A|/(1-\Delta) \rceil$, then the cost to the controller is*

$$J(e, d; j) = \left(1 - \frac{N_{cr}(1-\Delta)}{|A|}\right),$$

it is achievable by infinitely many binning and control strategies.

Proof: By the definition of N_{cr} in (5.16), there exists an encoding and decoding strategy pair $(e, d) \in \mathcal{S}_{(n, N_{cr}, t)}$ such that the codewords for the bins can be coded in such a manner that the two bins are $2t+1$ bits apart and t flips by jammer will have no effect on the decoded bin. Therefore, $\hat{\mathscr{Q}} = h(j(e(x))) = i$ for $x \in \mathcal{B}_i$. Using this in Lemma 5.5, we see that

$$P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{I} \right\} = \sum_{i=1}^{N} P\{x \in \mathcal{B}_i \cap \mathcal{T}_i'\},$$

which has to be minimized by the controller by choosing appropriate binning and control strategies. Recall that for $A > 0$

$$\mathcal{T}_i = \left[\frac{-1 + \Delta - u_i}{A}, \frac{1 - \Delta - u_i}{A}\right] \cap \mathcal{I}.$$

Now, construct bin $\mathcal{B}_i$ and $\mathcal{T}_i$ such that $\mathcal{T}_i \subseteq \mathcal{B}_i$ for all $i = 1, 2, ..., N_{cr}$ which implies $P\{x \in \mathcal{B}_i \cap \mathcal{T}_i'\} = \left(l(\mathcal{B}_i) - l(\mathcal{T}_i)\right)/2$ where $l(\cdot)$ is the length of the interval. Clearly,

$$\sum_{i=1}^{N_{cr}} l(\mathcal{B}_i) = 2 \quad \text{and} \quad \sum_{i=1}^{N_{cr}} l(\mathcal{T}_i) = N_{cr}\frac{2(1-\Delta)}{A}.$$

A simple calculation yields (holds for $A < 0$ also)

$$P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{I} \right\} = 1 - \frac{N_{cr}(1-\Delta)}{|A|},$$

which proves the theorem. There are multiple binning and control strategies which achieve this value by restricting $\mathcal{T}_i \subseteq \mathcal{B}_i$ for all $i = 1, 2, ..., N_{cr}$ and $l(\mathcal{B}_i) \geq 2\left(\frac{1-\Delta}{|A|}\right)$. ■

The set of strategies discussed in this section lead to a constructive upper bound on the cost $J(e, d; j)$ and $\gamma(n)$ for a given n. In the next section, we explore the possibility of reducing the cost by considering a game between the controller team and the jammer and solving for the saddle-point control and jamming strategies.

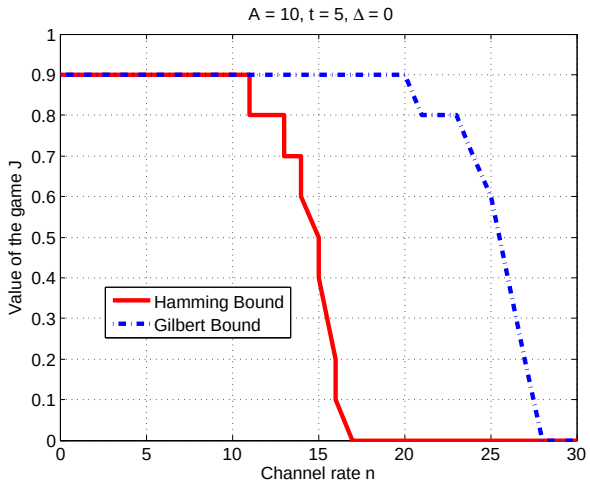


Figure 5.5: The change in value of the game $P\{x^+ \notin \mathcal{I} | x \in \mathcal{I}\}$ with increase in the channel rate n as obtained from Theorem 5.6 using the Hamming bound and the Gilbert bound. The simulation parameters are $A = 10$, $t = 5$, $\Delta = 0$. The actual cost lies between the two curves and depends on $n_{ecc}(N, t)$.

5.2.4 Saddle-Point Solution for the Two-Bin Case

Recall that when the channel rate $n < n_{ecc}(N, t)$ but $n \geq \log_2(N)$, then we need to compute $(e^*, d^*) \in \mathcal{E}_n \times \mathcal{D}_n$ and $j^* \in \mathcal{J}_{(t,n)}$ such that

$$J(e^*, d^*; j) \leq J(e^*, d^*; j^*) \leq J(e, d; j^*),$$

which holds for all $(e, d) \in \mathcal{E}_n \times \mathcal{D}_n$ and $j \in \mathcal{J}_{(t,n)}$. Consider the case when $A > 1$ and only one bit (i.e., $n = 1$) is available to the controller. The saddle-point solution for the jammer and the controller is derived in the following theorem.

Theorem 5.7 *Let $\epsilon \in \{0, 1\}$ be the received codeword at the decoder's end and $\hat{\mathcal{Q}} := h(\epsilon) = \epsilon$. For the game described above, the set of saddle-point solutions for the controller is given by*

$$u = \begin{cases} (A-1) + \lambda_1 A & \text{if } \hat{\mathcal{Q}} = 1, \\ -(A-1) - \lambda_2 A & \text{if } \hat{\mathcal{Q}} = 2, \end{cases}$$

with $\lambda_1, \lambda_2 \leq 0$ and $\lambda_1 + \lambda_2 = 2/A - 2$, and for the jammer, the probability that the jammer flips the bit is 1. The value of the game is

$$J(e^*, d^*; j^*) = 1 - \frac{1}{A}.$$

Proof: The cost function for the game is rewritten as

$$P\left\{x^+ \notin \mathcal{I} | x \in \mathcal{I}\right\} = P\left\{x^+ \notin \mathcal{I} | x \in \mathcal{B}_1\right\} P\left\{x \in \mathcal{B}_1 | x \in \mathcal{I}\right\} + P\left\{x^+ \notin \mathcal{I} | x \in \mathcal{B}_2\right\} P\left\{x \in \mathcal{B}_2 | x \in \mathcal{I}\right\}. \quad (5.17)$$

The quantity $P\{x^+ \notin \mathcal{I} | x \in \mathcal{B}_i\}$ is given by the expression

$$P\left\{x^+ \notin \mathcal{I} | x \in \mathcal{B}_i\right\} = \sum_{j=1}^{2} P\left\{x^+ \notin \mathcal{I} | x \in \mathcal{B}_i, \hat{\mathscr{Q}} = j\right\} P\left\{\hat{\mathscr{Q}} = j | x \in \mathcal{B}_i\right\}$$

for $i = 1, 2$. For notational simplicity, let us denote the $P\left\{\hat{\mathscr{Q}} = j | x \in \mathcal{B}_i\right\}$ by p_{ij}, which is the probability with which the jammer flips the bit corresponding to i^{th} bin to j^{th} bin. Now let us parameterize control values with the parameters λ_1, λ_2 such that

$$\begin{aligned} u_1 &= (A-1) + \lambda_1 A, \\ u_2 &= -(A-1) - \lambda_2 A. \end{aligned}$$

Let us separate the two bins at k, i.e. $\mathcal{B}_1 = [-1, k]$ and $\mathcal{B}_2 = (k, 1]$. Firstly, we need to compute the following quantities

$$\begin{aligned} P\left\{x^+ \notin \mathcal{I} | x \in \mathcal{B}_1, \hat{\mathscr{Q}} = 1\right\} &= 1 - P\left\{-1 \leq ax + u_1 \leq 1 | x \in \mathcal{B}_1, \hat{\mathscr{Q}} = 1\right\}, \\ &= 1 - P\left\{x \in \mathcal{T}_1 | \, x \in \mathcal{B}_1, \hat{\mathscr{Q}} = 1\right\}, \\ &= P\left\{x \in \mathcal{T}_1' \cap \mathcal{B}_1 | \, x \in \mathcal{B}_1, \hat{\mathscr{Q}} = 1\right\}, \end{aligned} \tag{5.18}$$

where $\mathcal{T}_1 = \left[-(1+\lambda_1), \left(\frac{2}{A} - 1 - \lambda_1\right)\right]$ and

$$\begin{aligned} P\left\{x^+ \notin \mathcal{I} | x \in \mathcal{B}_1, \hat{\mathscr{Q}} = 2\right\} &= 1 - P\left\{-1 \leq ax + u_2 \leq 1 | x \in \mathcal{B}_1, \hat{\mathscr{Q}} = 2\right\}, \\ &= P\left\{x \in \mathcal{T}_2' \cap \mathcal{B}_1 | \, x \in \mathcal{B}_1, \hat{\mathscr{Q}} = 2\right\}, \end{aligned} \tag{5.19}$$

where $\mathcal{T}_2 = \left[\left(1 + \lambda_2 - \frac{2}{A}\right), (1+\lambda_2)\right]$ and $\mathcal{T}' := \mathcal{I} \backslash \mathcal{T}$ denotes the complement of the set $\mathcal{T}$. It should be noted that the length of each $\mathcal{T}_i$ is $\frac{2}{A}$. By changing the values of λ_i, we are translating the set $\mathcal{T}_i$ within the interval $\mathcal{I}$ as shown in Figure 5.6.

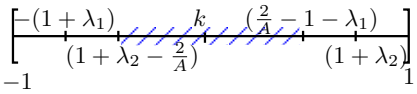


Figure 5.6: Two-bins case with $\lambda_1, \lambda_2 \leq 0$. The shaded portion denotes the indifference set $\mathcal{S} = \mathcal{T}_1 \cap \mathcal{T}_2$.

Now, consider the indifference set $\mathcal{S} := \mathcal{T}_1 \cap \mathcal{T}_2 \subseteq \mathcal{I}$ which is the set of points in $\mathcal{I}$ which remains within the bound $\mathcal{I}$ with both the control values u_1 and u_2. The indifference set is $\mathcal{S} = [1 + \lambda_2 - 2/A, 2/A - 1 - \lambda_1]$ if $-(1+\lambda_1) \leq 1 + \lambda_2 - 2/A$ or equivalently, $\lambda_1 + \lambda_2 \geq 2/A - 2$ and $\mathcal{S} = [-(1+\lambda_1), (1+\lambda_2)]$ if $\lambda_1 + \lambda_2 < 2/A - 2$ (see Figure 5.6).

With these notation and expressions, consider the case when $k \in \mathcal{S}$, $\lambda_1, \lambda_2 \leq 0$ and $\lambda_1 + \lambda_2 \geq 2/A - 2$. Then,

$$\begin{aligned}
P\left\{ x \in \mathcal{T}_1' \cap \mathcal{B}_1 \middle| x \in \mathcal{B}_1, \hat{\mathcal{Q}} = 1 \right\} &= \frac{-\lambda_1}{1+k}, \\
P\left\{ x \in \mathcal{T}_2' \cap \mathcal{B}_1 \middle| x \in \mathcal{B}_1, \hat{\mathcal{Q}} = 2 \right\} &= \frac{2 + \lambda_2 - 2/A}{1+k}, \\
P\left\{ x \in \mathcal{T}_1' \cap \mathcal{B}_2 \middle| x \in \mathcal{B}_2, \hat{\mathcal{Q}} = 1 \right\} &= \frac{2 + \lambda_1 - 2/A}{1-k}, \\
P\left\{ x \in \mathcal{T}_2' \cap \mathcal{B}_2 \middle| x \in \mathcal{B}_2, \hat{\mathcal{Q}} = 2 \right\} &= \frac{-\lambda_2}{1-k}.
\end{aligned}$$

Substituting $p_{11} = 1 - p_{12}$ and $p_{22} = 1 - p_{21}$ yields,

$$\begin{aligned}
P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{B}_1 \right\} &= \frac{-\lambda_1}{1+k} + p_{12} \frac{2 + \lambda_1 + \lambda_2 - 2/A}{1+k}, \\
P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{B}_2 \right\} &= \frac{-\lambda_2}{1-k} + p_{21} \frac{2 + \lambda_1 + \lambda_2 - 2/A}{1-k}.
\end{aligned}$$

Substituting this in (5.17), we get

$$P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{I} \right\} = -\frac{\lambda_1 + \lambda_2}{2} + (p_{12} + p_{21}) \left(1 + \frac{\lambda_1 + \lambda_2}{2} - \frac{1}{A} \right), \tag{5.20}$$

with $\lambda_1, \lambda_2 \leq 0$, $\lambda_1 + \lambda_2 \geq 2/A - 2$ and $p_{12}, p_{21} \in [0, 1]$. The inf sup of the game is

$$\begin{aligned}
\inf_{\lambda_1, \lambda_2} \sup_{p_{12}, p_{21}} P\left\{ x^+ \notin \mathcal{I} \middle| x \in \mathcal{I} \right\} &= \inf_{\lambda_1, \lambda_2} 2 - \frac{2}{A} + \frac{\lambda_1 + \lambda_2}{2} \\
&= 1 - \frac{1}{A}.
\end{aligned}$$

The supremum is attained with $p_{12} = p_{21} = 1$ and $\lambda_1 + \lambda_2 = 2/A - 2$. The sup inf of the game also yields the same result, and therefore, it is the value of the game and $p_{12} = p_{21} = 1$ and $\lambda_1 + \lambda_2 = 2/A - 2$ is the saddle-point strategy. Similarly, the case of $\lambda_1 + \lambda_2 < 2/A - 2$ has the same value as above, but is attained for $\lambda_1 + \lambda_2 = 2/A - 2$ which can only be achieved with an ϵ-saddle-point strategy. Hence, this equilibrium is ruled out to be a saddle-point solution to the game.

If $k \notin \mathcal{S}$, then the cost function is strictly greater than the one computed in (5.20). Therefore, the saddle-point value of the game for the case of $k \notin \mathcal{S}$ is also greater than the one in (5.20) and is ruled out as a saddle-point solution to the game.

For the case of $\lambda_1, \lambda_2 \geq 0$, the inf sup and sup inf of the game comes out to be $2 - 2/A$ with $\lambda_1 = \lambda_2 = 0$ for $A \leq 2$ and 1 for $A > 2$, which is higher than the value calculated above. Therefore, that will not be a saddle-point solution. ∎

Geometrically, the two indifference intervals $[-(1+\lambda_1), (1+\lambda_2)]$ and $[1 + \lambda_2 - 2/A, 2/A - 1 - \lambda_1]$ coincide at the saddle-point strategy of the controller. Therefore, the controller is trying to maximize the indifference interval by appropriately choosing the values of λ_1 and λ_2 and the jammer is flipping the bit every time.

5.2.5 Analysis for the N-Bin Case

Let us assume that there are N bins $\mathcal{B}_i,\ i \in \mathscr{J} = \{1, \cdots, N\}$ and the system has process noise. We can get an idea of the saddle-point solution to the game using Lemma 5.5. The value of the game is defined if the inf sup is equal to the sup inf of the cost function [33]. The inf sup for this game is

$$\inf_{u_i, 1\le i\le N} \sup_{\substack{p_{ik},\ k\in\mathscr{N}_i,\\ \sum_{k\in\mathscr{N}_i} p_{ik}=1}} \sum_{i=1}^{N} \sum_{k\in\mathscr{N}_i} p_{ik} P\{x \in \mathcal{B}_i \cap \mathcal{T}_k'\} = \inf_{u_i, 1\le i\le N} \sum_{i=1}^{N} \sup_{k\in\mathscr{N}_i} P\{x \in \mathcal{B}_i \cap \mathcal{T}_k'\}, \tag{5.21}$$

where the supremum is attained by

$$p_{ik} = \begin{cases} 1 & \text{if } k = \arg\sup_{l\in\mathscr{N}_i} P\{x \in \mathcal{B}_i \cap \mathcal{T}_l'\}, \\ 0 & \text{otherwise.} \end{cases} \tag{5.22}$$

i.e., the jammer always flips the bits in such a manner, so as to produce the codeword for k which has least overlap between $\mathcal{B}_i$ and $\mathcal{T}_k$. If $\arg\sup_{l\in\mathscr{N}_i} P\{x \in \mathcal{B}_i \cap \mathcal{T}_l'\}$ is a set with more than one element, then the jammer has uniform probability over the entire set.

The sup inf can also be computed for this game, but is dependent on the set $\mathscr{N}_i$. The quantity in (5.21) gives the upper bound on the value of the game [33]. If inf sup of the cost function is equal to the sup inf (subject to the constraint (5.15)), then saddle-point exist and the jammer's strategy is given by (5.22).

At this point, it is a natural question to ask if the cost can be driven to zero even if $n < n_{ecc}(N, t)$. We will use rate distortion theory to find an answer to this question in the next section. This gives us a lower bound on $n^\star$.

5.3 A Lower Bound using Rate Distortion Theory

In this section, we use information theory to find the minimum number of bits (the ultimate lower bound) required to control the plant reliably in the presence of the jammer. Our problem can be posed as a rate distortion problem [38], which is widely studied in the field of information theory. The key observation here is that the controller needs the value of the state (and not that of quantization bin) in order to compute the control value for the plant. In order to keep the state within the interval $\mathcal{I}$, the controller needs the information about the state within an error of $(1-\Delta)/|A|$. Therefore, the maximum allowable difference between the state of the plant x and the estimate of the state $\hat{x}$ must be less than $(1-\Delta)/|A|$. With this idea, we can provide a lower bound (albeit loose) on the number of bits using rate distortion theory. The following lemma will establish the connection between our original problem and information theory.

Lemma 5.8 *Consider the problem formulated in Section 5.1. The cost $P\{x^+ \notin \mathcal{I} | x \in \mathcal{I}\}$ is zero for all jamming strategies if and only if there exists encoding and decoding policies such that*

$$\sup_{p(j|e)} |x - \hat{x}| \le \frac{1-\Delta}{|A|} \quad \textit{for almost all } x \in \mathcal{I}. \tag{5.23}$$

Proof: If the inequality in (5.23) holds for some encoding and decoding policy pair, then the controller can send $u = -A\hat{x}$ which keeps the state $|x^+| = |Ax - A\hat{x}| \leq 1 - \Delta$ within the interval $\mathcal{I}$.

Now, if the value of the game is zero for all jamming strategies, then $|Ax + u| \leq 1 - \Delta$ for some encoding and decoding policy and for all $x \in \mathcal{I}$. Pick $\hat{x} = -u/A$. Since this holds for all jamming strategies, we get $\sup_{p(j|e)} |x - \hat{x}| \leq (1 - \Delta)/|A|$. ∎

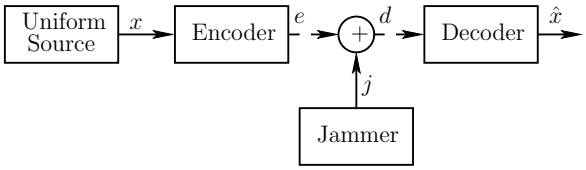


Figure 5.7: An equivalent representation of the control problem posed as a communication problem with distortion.

This problem is different in three ways from the one usually studied in information theory. First, due to the constraint on the number of bits to transfer the state information, our result does not rely on results with arbitrarily large codelength. Second, we are sending a real number over a channel with finite codelength and some information is lost in encoding the real number. Third difference is the presence of a jammer, who is observing the input codewords and strategically flipping the bits in order to alter the estimate of the state. Therefore, the distortion in this case has to take care of both, the jammer and the information lost due to encoding a real number. Now, let us define distortion function as

$$d(x, \hat{x}) = (x - \hat{x})^2,$$

whose expected value is to be minimized by the controller by choosing $p(\hat{x}|x)$ and maximized by the jammer by choosing $p(j|e)$. The distortion rate function is defined as

$$D(R) = \inf_{\substack{p(\hat{x}|x) \\ I(X;\hat{X}) \leq R}} E_X\{d(X; \hat{X})\},$$

where $I(X; \hat{X})$ is the mutual information between the random variables X and $\hat{X}$ (see [38] for the definition of mutual information). The following theorem characterizes the minimum value of the rate n, say $n_{rdt}(A, \Delta, t)$, for the system to have zero cost in terms of distortion rate function. It must be noted that if $n < n_{rdt}(A, \Delta, t)$, then there is no encoding-decoding policy whatsoever which can ensure zero cost to the controller.

Theorem 5.9 *If the value of the game $J(e, d; j)$ is zero for some encoding and decoding policy pair $(e, d) \in \mathcal{E}_n \times \mathcal{D}_n$ and for all jamming strategies $j \in \mathcal{J}_{(t,n)}$, then n satisfies*

$$D(C_J(n,t)) \quad \leq \quad \frac{(1-\Delta)^2}{A^2}, \tag{5.24}$$

$$\text{where } C_J(n,t) \quad := \quad n - \log_2 \left(\sum_{i=0}^{t} \binom{n}{i} \right). \tag{5.25}$$

Proof: From Lemma 5.8, if the value of the game is zero, then there exists an encoding and decoding policy pair such that $\sup_{p(j|e)} d(x, \hat{x}) \leq \frac{(1-\Delta)^2}{A^2}$ for almost all $x \in \mathcal{I}$. Now assume that the jammer fixes its strategy

such that it flips $i \leq t$ bits at random with uniform probability. Then, there exists an encoding-decoding policy pair such that the $E_X\{d(X,\hat{X})\} \leq \frac{(1-\Delta)^2}{A^2}$. With this jamming strategy, the mutual information is bounded by

$$\begin{aligned} I(X;\hat{X}) &\leq I(e;d) = H(d) - H(d|e) \\ &\leq n - H(j|e) = C_J(n,t), \end{aligned}$$

where the first inequality holds due to data processing inequality [38] and the second inequality holds by taking uniform distribution over the received bits at decoder. Hence, there exists an $\hat{x}$ such that $I(X;\hat{X}) \leq C_J(n,t)$ and $E_X\{d(X,\hat{X})\} \leq \frac{(1-\Delta)^2}{A^2}$ for almost all $x \in \mathcal{I}$. As a result, we get

$$D(C_J(n,t)) = \inf_{\substack{p(\hat{x}|x),\\ I(X;\hat{X}) \leq C_J(n,t)}} E_X\{d(X;\hat{X})\} \leq \frac{(1-\Delta)^2}{A^2}.$$

■

Hence, the jammer chooses the strategy which minimizes the mutual information and then the encoder and decoder minimize the mean-squared distortion by choosing appropriate $p(\hat{x}|x)$. This gives a necessary condition on the number of bits n required by the controller to achieve the required distortion as derived in Lemma 5.8 which ensures zero cost. It is clear that $n_{rdt}(A,\Delta,t) \leq n_{ecc}(N,t)$, but to ascertain the tightness of $n_{ecc}(N,t)$, numerical simulations are done to find the value of $n_{rdt}(A,\Delta,t)$ and check the difference $n_{ecc}(N,t) - n_{rdt}(A,\Delta,t)$. The following lower bound on rate-distortion function [39] can be used to compute $n_{rdt}(A,\Delta,t)$:

$$R(D) \geq \frac{1}{2}\log_2\left(\frac{4}{2\pi e D}\right).$$

This gives the lower bound on the channel rate $R(D)$ at which expected mean-squared distortion D is achieved for a uniform source taking values in the interval $[-1,1]$ for all codelengths. Substituting $R(D) = C_J(n,t)$, we get a lower bound on the distortion D :

$$\frac{2}{\pi e 2^{2C_J(n,t)}} \leq D(C_J(n,t)) \leq \frac{(1-\Delta)^2}{A^2}.$$

The minimum n for which this inequality holds gives us a lower bound on $n_{rdt}(A,\Delta,t)$. Substituting the value of $C_J(n,t)$ from (5.25) and rearranging, we see that

$$\frac{|A|}{(1-\Delta)} \leq \sqrt{\frac{\pi e}{2}} \frac{2^n}{\left(\sum_{j=0}^{t} \binom{n}{j}\right)},$$

which is a restatement of the Hamming bound with a multiplicative constant $\sqrt{\frac{\pi e}{2}} \approx 2.1$. As a result of this, $n_{rdt}(A,\Delta,t) \leq n_{Hamming}(N,t)$.

The following theorem summarizes the main result of the chapter and gives the necessary and sufficient condition on $n^\star$ for $\gamma(n) = 0$ for the original problem formulated in Section 5.1.

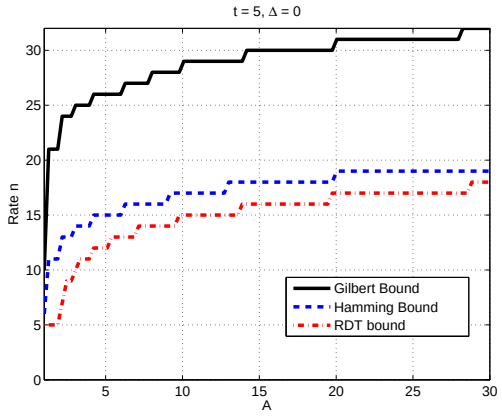


Figure 5.8: A plot of rate n obtained from Theorem 5.4 using the Hamming bound and the Gilbert bound and necessary condition on rate n obtained from Theorem 5.9 using rate distortion theory (RDT) for the controller to incur zero cost as a function of A. The simulation parameters are $t = 5$ and $\Delta = 0$.

Theorem 5.10 *Consider the problem formulated in Section 5.1 where the jammer can flip at most t bits in the codeword. Recall that $n^\star = \min\{n \in \mathbb{N} : \gamma(n) = 0\}$, $n_{rdt}(A, \Delta, t)$ satisfies*

$$n_{rdt}(A,\Delta,t) = \min\left\{ n \in \mathbb{N} : \frac{|A|}{(1-\Delta)} \leq \sqrt{\frac{\pi e}{2}} \frac{2^n}{\left(\sum_{j=0}^{t} \binom{n}{j}\right)} \right\},$$

and $N = \lceil |A|/(1-\Delta) \rceil$. Then $n^\star$ satisfies

$$n_{rdt}(A,\Delta,t) \leq n^\star \leq n_{ecc}(N,t) \leq n_{Gilbert}(N,t).$$

Proof: Follows from the discussion up to this point. ∎

5.4 Summary

We considered a deception attack on a networked control system in the presence of an intelligent and strategic jammer, which flips at most t bits in the observation codeword. We restricted our attention to binning based control strategy to obtain an upper bound on the cost to the controller and a sufficient condition on the codelength required to drive the cost to zero. We then posed the problem as a zero-sum game between the team of encoder-decoder-controller and the jammer for the case when the codelength is small. We derived the saddle-point strategy for the controller and the jammer for the case when the jammer can flip one bit and the controller has one bit to transfer state information. We derived a necessary and sufficient condition on the channel rate n for which the cost is zero, i.e., state leaves the bounded set $\mathcal{I}$ with probability zero.

Note that in this chapter, we focused our attention to one stage control system. We would like to extend the result to a dynamic system, which evolves over time. This will be addressed in our future work.

CHAPTER 6

CONCLUSION

In this thesis, we considered three problems related to security attacks on networked control systems in the presence of a strategic but action-limited jammer potentially disrupting the communication between the controller and the plant. This led to a zero-sum dynamic game for which we established the existence of saddle-point equilibrium strategies.

At first, we considered optimal control of discrete time LTI scalar systems under a denial of service attack by a jammer for the two cases - when there is a constraint on the observation and when the observation is unconstrained. The jammer can block the control signal at each time step, but has limited number of chances to do so over the entire horizon. In the case where the jammer can only act once over the decision horizon, we proved that its strategy is threshold-based, and characterized the behavior of the threshold in the large state limit. We presented the result for the more general case and touched upon the case when the system is multi-dimensional.

Next, we considered a deception attack on a one-step control system. The system considered was a scalar linear discrete time system with only one step to control. The cost function considered is the probability that the state leaves a bounded set in the next time step. We obtained a sufficient condition on number of bits required to achieve zero cost and a constructive upper bound on the cost function by restricting the encoder, decoder and the controller to use binning-based control strategies. We obtained a necessary condition on the number of bits required to achieve zero cost using tools from rate distortion theory. We also proved the existence of saddle-point strategies for the system when the number of bits is smaller than the sufficient number of bits required for keeping the state bounded in the next time step; we also obtained the saddle-point strategy for the case when the controller is restricted to use one bit to transfer the observation information.

6.1 Future Work

Future work can take different directions. Since the analyses for general cases are difficult, efficient computational methods need to be developed to compute approximate policies. One possible approach is to use rolling horizon control, such that the total number of the instances when the jammer acts in the entire horizon is still limited by M. One can also switch to efficient computational methods to compute or approximate the set of states at which the jammer jams, possibly using ideas from approximate dynamic programming.

As we inferred from the study, the jammer can launch attacks which affect the information available at the controller. In a multi-agent scenario, such attacks can have a deleterious effect on the performance of the control system. Attack on information structure due to jamming will require the concepts from team

theory as well as communication theory, and it will be exciting to see various concepts leading to a new class of problems being solved.

Another extension of the work can be to extend the result of Chapter 5 to a dynamic setting, where the codelength is constrained in the presence of the jammer. It will be interesting to obtain the minimum codelength at which the state remains bounded with probability one. The optimal binning and control strategies may also evolve over time in such a scenario.

CHAPTER 7

REFERENCES

[1] S. Tatikonda and S. Mitter, "Control under Communication Constraints," *IEEE Transactions on Automatic Control*, vol. 49, no. 7, pp. 1056–1068, 2004.

[2] G. Nair, F. Fagnani, S. Zampieri, and R. Evans, "Feedback control under data rate constraints: an overview," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 108–137, 2007.

[3] S. Yüksel and T. Başar, "Minimum Rate Coding for LTI Systems over Noiseless Channels," *IEEE Transactions on Automatic Control*, vol. 51, no. 12, pp. 1878–1887, 2006.

[4] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. Sastry, "Foundations of control and estimation over lossy networks," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 163–187, 2007.

[5] O. Imer, S. Yüksel, and T. Başar, "Optimal control of LTI systems over unreliable communication links," *Automatica*, vol. 42, no. 9, pp. 1429–1439, 2006.

[6] E. Garone, B. Sinopoli, and A. Casavola, "LQG control over lossy TCP-like networks with probabilistic packet acknowledgements," *International Journal of Systems, Control and Communications*, vol. 2, no. 1, pp. 55–81, 2010.

[7] P. Antsaklis and J. Baillieul, "Special issue on technology of networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 5–8, 2007.

[8] C. Hadjicostis, C. Langbort, N. Martins, and S. Yüksel, "Special issue on information processing and decision making in distributed control systems," *Int. Journal of Systems, Control, and Communications*, vol. 2, no. 1/2/3, 2010.

[9] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. Jordan, and S. Sastry, "Kalman Filtering with Intermittent Observations," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1453–1464, 2004.

[10] T. Katayama, "On the matrix Riccati equation for linear systems with random gain," *Automatic Control, IEEE Transactions on*, vol. 21, no. 5, pp. 770–771, 1976.

[11] S. Amin, A. Cárdenas, and S. Sastry, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks," *Hybrid Systems: Computation and Control*, pp. 31–45, 2009.

[12] H. Sandberg, A. Teixeira, and K. Johansson, "On security indices for state estimators in power networks," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, 2010.

[13] A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the 3rd conference on Hot topics in security*, 2008, pp. 1–6.

[14] S. Gorman, Y. J. Dreazen, and A. Cole, "Insurgents hack U.S. drones," December 2009, http://online.wsj.com/article/SB126102247889095011.html.

[15] P. Marks, "Stuxnet: the new face of war," *The New Scientist*, vol. 208, no. 2781, pp. 26–27, 2010.

[16] T. Chen, "Stuxnet, the real start of cyber warfare?" *IEEE Network*, vol. 24, no. 6, pp. 2–3, 2010.

[17] P. Bommannavar and T. Başar, "Optimal control with limited control actions and lossy transmissions," in *47th IEEE Conference on Decision and Control (CDC)*, 2008, pp. 2032–2037.

[18] O. Imer and T. Başar, "Optimal control with limited controls," in *Proceedings of the 2006 American Control Conference*. Citeseer, 2006, pp. 298–303.

[19] O. Imer and T. Başar, "Optimal estimation with limited measurements," *Int. J. Systems, Control, and Communications (Special Issue on Information Processing and Decision Making in Distributed Control Systems)*, vol. 2, no. 1/2/3, pp. 5–29, 2010.

[20] V. Borkar and S. Mitter, "LQG control with communication constraints," *Laboratory for Information and Decision Systems, Massachusetts Institute of Technology*, 1995.

[21] R. Bansal and T. Başar, "Simultaneous design of measurement and control strategies for stochastic systems with feedback," *Automatica*, vol. 25, no. 5, pp. 679–694, 1989.

[22] H. Witsenhausen, "Separation of estimation and control for discrete time systems," *Proceedings of the IEEE*, vol. 59, no. 11, pp. 1557–1566, 1971.

[23] Y. Bar-Shalom and E. Tse, "Dual effect, certainty equivalence, and separation in stochastic control," *IEEE Transactions on Automatic Control*, vol. 19, no. 5, pp. 494–500, 1974.

[24] D. Bertsekas, *Dynamic Programming and Optimal Control, vol. I & II*. Athena Scientific, 2007.

[25] G. Nair and R. Evans, "Stabilizability of stochastic linear systems with finite feedback data rates," *SIAM Journal on Control and Optimization*, vol. 43, no. 2, pp. 413–436, 2005.

[26] S. Yüksel and T. Başar, "Control over noisy forward and reverse channels," *IEEE Transactions on Automatic Control*, no. 99.

[27] T. Başar, "The Gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, 1983.

[28] A. Kashyap, T. Başar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2119–2123, 2004.

[29] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2005, pp. 46–57.

[30] "Monster solar flare jams radio signals," February 2011, http://news.discovery.com/space/solar-flare-radio-communications-disruption-110217.html.

[31] R. Turk, *Cyber incidents involving control systems*. Idaho National Engineering and Environmental Laboratory, 2005.

[32] E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems," in *Proceedings of the VDE Kongress*, vol. 116, 2004.

[33] T. Başar and G. Olsder, *Dynamic Noncooperative Game Theory*. Society for Industrial Mathematics (SIAM) Series in Classics in Applied Mathematics, Philadelphia, 1999.

[34] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *49th IEEE Conference on Decision and Control (CDC)*, December 2010, pp. 1096–1101.

[35] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, New York, USA, 2004.

[36] A. Gupta, P. Grover, C. Langbort, and T. Başar, "One-Stage control over an adversarial channel with finite codewords," in *Submitted to IEEE Conference on Decision and Control*, 2011.

[37] S. Wicker, *Error Control Systems for Digital Communication and Storage*. Prentice Hall, New Jersey, 1995.

[38] T. Cover and J. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.

[39] S. Azami, O. Rioul, and P. Duhamel, "Performance bounds for joint source-channel coding of uniform memoryless sources using a binary decomposition," in *Proceedings of European Workshop on Emerging Techniques for Communication Terminals*, 1997, pp. 259–263.